

DEFENSE LOGISTICS AGENCY

HEADQUARTERS
CAMERON STATION
ALEXANDRIA, VIRGINIA 22314

DLA-NS

3 Oct 77 **

FOREWORD

This manual is issued under the directional authority of, and in accordance with Department of Defense Directive 5220.22, Department of Defense Industrial Security Program. It establishes uniform security practices within industrial plants, educational institutions, and all organizations and facilities used by prime and subcontractors having classified information of the Department of Defense, certain other Executive Departments and Agencies, or certain foreign governments. Users of this publication are encouraged to submit recommended changes and comments to improve the publication, through channels, to HQ DLA, ATTN: DLA-N.

This revision is required by the demands of national security as determined by the Government. It is issued pursuant to and constitutes notice prescribed by section 1A (i) of the Department of Defense Security Agreement (DD Form 441), and section 1A of the Department of Defense Transportation Security Agreement (DLA Form 1149).

This manual shall be effective 3 October 1977.

FOR THE DIRECTOR

J. J. McALEER, JR.
for J. J. McALEER, JR.
Colonel, USA
Staff Director, Administration

DISTRIBUTION

Defense Logistics Agency: 2 less DPDOs

Army:

Active Army: To be distributed in accordance with DA Form 12-9A requirements for Security—D.

USAR & ARNG: NONE

SUMMARY OF CHANGES

The following is a brief description of changes, by paragraph. Some paragraphs contain only editorial revisions and therefore are not enumerated. DCAS-DD has been redesignated DLA-DD(CAS). This and other type editorial corrections have not been identified. The text of this manual identifies all DLA forms as such; however, illustrations of forms in appendix I will retain the DSA identification until such time as the forms are reprinted.

1. A listing of the changed paragraphs follows:

Paragraph

- | | |
|------------------------|--|
| 3bb | Modified to clarify definition of Representative of Foreign Interest. |
| 5s | Modified to permit a parent-subsidiary organization to publish an SPP applicable throughout the organization but adapted to be applicable at specific operating locations. Also, provision has been added in the case of one-person facilities that the cognizant security office be advised of the current combination of the container. Where the one-person facility is a part of a multiple facility organization, the home office facility security supervisor is to be advised of the current combination. |
| Footnote 10 to Par. 5u | Laos is now considered to be a Communist country. |
| 6b(1) & (2) | Eliminate reference to OSE procedures and reference a new procedure whereby contractor employees will be issued Letters of Consent or Security Assurances. Also include provision for reporting regarding an individual who has taken residence or assignment outside the U.S. for a period in excess of 90 consecutive days during any 12-month period. |
| 6b(6) | Requires a report for a cleared immigrant alien who has been assigned or taken residence outside the U.S. for a period in excess of 90 calendar days in any 12-month period. Visits in excess of 90 days invalidate any existing clearance. |
| 14f & g | Permits use of repaired security cabinets for the storage of CONFIDENTIAL or the storage of SECRET with supplemental controls, and outlines measures to be used in effecting repairs, and records to be maintained pertinent to such cabinets. |
| 19b(2) | Requires contracting officer approval for destruction of accountable COMSEC vice CRYPTO. |
| 19d | Permits subcontractor guard to be a witness to destruction of CONFIDENTIAL material, other than accountable COMSEC, provided the guard is employed full-time, is under the supervision and direction of the facility security supervisor, possesses an appropriate clearance, has been briefed and is designated to witness the destruction. |
| 19f | Permits subcontractor guard to destroy CONFIDENTIAL waste, except CRYPTO or other Special Access information. |

Paragraph

- 20f Deletes reference to the "OSE determination" and substitutes Letter of Consent or Security Assurance.
- 20m Now permits short-term visits of not more than 90 days by immigrant aliens without negating the basis upon which the Letter of Consent is issued.
- 28 Deletes requirement for contractor to maintain record of employees who have been granted an OSE determination.
- 29a Permits contractor to administratively terminate contractor granted CONFIDENTIAL clearances.
- 29d Sets forth debriefing procedures in the case of contractor granted CONFIDENTIAL clearances which are administratively terminated and specifies 2-year retention period for DLA Forms 683 and 482 in such cases.
- 48c Deletes "OSE determination".
- 48e Now requires that visit requests processed through DISCO be submitted in duplicate (formerly quadruplicate) with an extra copy for each additional country to be visited.
- 50 Deletes "OSE determination".
- 72b Amends last sentence to call attention to exceptions set forth in paragraph 5x.
- 72c Now permits two or more cleared facilities (occupying the same office space or located side by side) consisting of a parent and one or more wholly owned subsidiaries to utilize common security services for: (i) personnel security administration, (ii) document control (including storage), (iii) reproduction, (iv) visitor control, and (v) other similar administrative services. Also outlines SPP coverage necessary in such circumstances.
- Section XII Complete rewrite to eliminate OSE concept and substitute procedures whereby contractor employees who require access to classified information will be issued Letters of Consent or Security Assurances while stationed outside the U.S. The new address for OISE is included in this rewrite (paragraph 95c). Changed language in this section not identified by marginal arrows.
- Appendix I Deletes reference to OSE determination. Introduces new DISCO Form 382 and deletes DLA Forms 382-R and 383-R.

Glossary of Acronyms and Abbreviations Commonly Used in the Defense Industrial Security Program

ACO	Administrative Contracting Officer
ACDA	U.S. Arms Control and Disarmament Agency
ACSI	Assistant Chief of Staff for Intelligence, Department of Army
ADP	Automatic Data Processing
ADS	Advanced Declassification Schedule
AMSP	Allied Military Security Publication
APO	Army Post Office
ARFCOS	Armed Forces Courier Service
ASD(A)	Assistant Secretary of Defense (Administration)
ASD(C)	Assistant Secretary of Defense (Comptroller)
ARPC	Air Reserve Personnel Center
ASPR	Armed Services Procurement Regulation
BI	Background Investigation
BL	Bill(s) of Lading
(C)	CONFIDENTIAL
CAB	Civil Aeronautics Board
CBL	Commercial Bill(s) of Lading
CDSS	Canadian Department of Supply and Services
CENTO	Central Treaty Organization
CM	Candidate Material
COMINT	Communications Intelligence
COMSEC	Communications Security
CONUS	Continental United States
COR	Central Office of Record
COSMIC—	Property NATO and Subject to Special Security Controls
TOP SECRET	
CSC	Civil Service Commission
CSISM	COMSEC Supplement to the Industrial Security Manual
CSO	Cognizant Security Office
DASD(SP)	Deputy Assistant Secretary of Defense (Security Policy)
DCASR	Defense Contract Administration Services Region
DCII	Defense Central Index of Investigations
DDC	Defense Documentation Center
DIA	Defense Intelligence Agency
DIS	Defense Investigative Service
DISCO	Defense Industrial Security Clearance Office
DISI	Defense Industrial Security Institute
DLA	Defense Logistics Agency
DLA-DD(CAS)	Deputy Director, Contract Administration Services, Defense Logistics Agency
DNACC	Defense National Agency Check Center

DoD	Department of Defense
DoDAAD	Department of Defense Address Directory
DOT	Department of Transportation
EDIS	Executive Directorate, Industrial Security (formerly OIS)
ENAC	Expanded National Agency Check
E.O.	Executive Order
EPA	Environmental Protection Agency
ERDA	Energy Research and Development Agency (formerly AEC)
FAA	Federal Aviation Agency (Presently Federal Aviation Administration, Department of Transportation)
FBI	Federal Bureau of Investigation
FEA	Federal Energy Administration
FOCI	Foreign Ownership, Control and Influence
(FRD)	FORMERLY RESTRICTED DATA
FSC	Federal Supply Code
FSS	Federal Supply Schedule
GBL	Government Bill(s) of Lading
GDS	General Declassification Schedule
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GPO	Government Printing Office
GSA	General Services Administration
HEW	Department of Health, Education and Welfare
HOF	Home Office Facility
HQ DLA	Headquarters Defense Logistics Agency
HQ DLA-N	Headquarters Defense Logistics Agency, Executive Directorate, Industrial Security
ICC	Interstate Commerce Commission
IFB	Invitation for Bid
IPO	International Pact Organization
ISB	Industrial Security Bulletin
ISCRO	Industrial Security Clearance Review Office
ISL	Industrial Security Letter
ISM	Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M)
ISR	Industrial Security Regulation (DoD 5220.22-R)
ITAR	International Traffic in Arms Regulations
KGB	Committee of State Security (Soviet Union)
MAAG	Military Assistance Advisory Group
MAP	Mutual Aid Program
MDAP	Mutual Defense Assistance Program
MIL-STD	Military Standard (Book Form)
MTMC	Military Traffic Management Command (formerly MTMTS)
N/A	Not Applicable
NAC	National Agency Check

NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NIS	Naval Investigative Service
NPLO	NATO Production Logistics Organization
NSA	National Security Agency
NSF	National Science Foundation
OASD(A)	Office of the Assistant Secretary of Defense (Administration)
OASD(C)	Office of the Assistant Secretary of Defense (Comptroller)
OASD(PA)	Office of the Assistant Secretary of Defense (Public Affairs)
ODC	Office of Defense Cooperation
OISE	Office of Industrial Security, Europe
ODEPs	Owners, Officers, Directors, Partners, Regents, Trustees, or Executive Personnel
OSD	Office of Secretary of Defense
OSI	Office of Special Investigations, USAF
PCO	Procuring Contracting Officer
PMF	Principal Management Facility
PRP	Personnel Reliability Program
PSCF	Personnel Security Clearance Files
PSQ	Personnel Security Questionnaire
PSS	Protective Security Service
(RD)	RESTRICTED DATA
RFP	Request for Proposal
RFQ	Request for Quote
(S)	SECRET
SBA	Small Business Administration
SEATO	Southeast Asia Treaty Organization
SIOP	Single Integrated Operational Plan
SPP	Standard Practice Procedure
SSS	Signature Security Service
T.O.	Transportation Officer
(TS)	TOP SECRET
TSEC	U.S. Telecommunications Security
TWX	Teletype Communications
(U)	UNCLASSIFIED
U.K.	United Kingdom
UL	Underwriters' Laboratories
U.S.	United States
USACSLA	U.S. Army Communications Security Logistics Agency
USAFSS	U.S. Air Force Security Service
USAINTC	U.S. Army Intelligence Command
USASA	U.S. Army Security Agency
USASTRATCOM	U.S. Army Strategic Communications Command
USC	United States Code
USCSB	U.S. Communications Security Board
USIB	U.S. Intelligence Board

CH 1 Approved For Release 2002/08/21 : CIA-RDP94B01041R000300040001-2
DoD 5220.22-M

VA	Veterans Administration
XCL	Excluded from the General Declassification Schedule
XGDS	Exempt from the General Declassification Schedule

CONTENTS

SECTION I. GENERAL

Paragraph	Page
1 Scope	1
2 Applicable Federal Statutes, Executives Orders, and Regulations	2
3 Definitions.....	2
4 Designation of Cognizant Security Office	9
5 General Requirements	10
6 Reports	20
7 Loss, Compromise, or Suspected Compromise of Classified Information.....	26
8 Badges and Identification Cards	27
9 DoD Sponsorship of Meetings	28

SECTION II. HANDLING OF CLASSIFIED INFORMATION

11 Marking	33
10 Classification	35
12 Record of Classified Material	43
13 Special Requirements for TOP SECRET	45
14 Storage	46
15 Alternate Storage Locations	50
16 Safeguards During Use	51
17 Transmission	51
18 Reproduction	60
19 Destruction	61

SECTION III. SECURITY CLEARANCES

20 General	65
21 Facility Security Clearances	68
22 Personnel Clearances Required in Connection with Facility Clearances ..	69
23 Security Clearance of Negotiators	74
24 Security Clearance of Additional Personnel	74
25 Preemployment Clearance Application—Prohibited	76
26 Application for Personnel Security Clearance	77
27 Clearance of Present and Former Civilian and Military Personnel of the DoD and Certain Other Government Agencies	83
28 Contractor's Clearance Record	84
29 Administrative Termination of Personnel Security Clearances	85
30 Administrative Downgrading of TOP SECRET Personnel Security Clearances .	86
31 Canadian and U.K. Reciprocal Clearances	87

Paragraph

Page

SECTION IV. CONTROL OF AREAS

32	Purpose	89
33	General	89
34	Area Controls	89
35	Supplemental or Supplanting Alarm Systems.....	91
36	Supplanting and Supplemental Electronic, Mechanical and Electro-Mechanical Access Control Devices	92

SECTION V. VISITOR CONTROL PROCEDURES

Part 1. Visits to User Agency Contractors

37	General	95
38	Identification and Control of Visitors	96
39	Visitor Record	97
40	Long-Term Visitors	98
41	Visitor Categories and Procedures	98
42	Visits Involving Access to RESTRICTED DATA	100

Part 2. Visits to User Agency Activities

43	General Rules—In Addition to Paragraph 37	103
44	Visits to User Agency Activities in the U.S.....	103
45	Visits to User Agency Activities Outside the U.S.	104

Part 3. Visits to Government Activities Other Than User Agencies

46	Visits to ERDA Installations or ERDA Contractors	104
47	Visits to Activities Other Than ERDA	105

Part 4. Visits to Foreign Governments and Activities

48	General	105
49	Processing Time	106
50	Use of OISE	107

*Part 5. Visits in Connection With Bilateral Industrial Security Agreements
and NATO Visit Procedures*

51	Visits in Connection with Bilateral Industrial Security Agreements.....	107
52	NATO Visit Procedures	107
53	NPLO Programs Clearance and Visit Procedures	108
54	Records of NATO Visits	109
55	Certificate of Security Clearance	109

SECTION VI. SUBCONTRACTORS, VENDORS, AND SUPPLIERS

56	Application to Subcontractors	111
57	Application to Sub-Subcontractors	111

Paragraph	Page
58 Determination of Clearance Status	111
59 Safeguarding Ability	111
60 Classification Guidance	112
61 Required Distribution	115
62 Notification of Selection	116
63 Unsatisfactory Security Conditions	116
64 Return of Classified Information	116
65 Subcontracting With Foreign Industry	116
66 Subcontracts Arising From Foreign Classified Contracts	116

SECTION VII. CONSULTANTS

67 General	119
68 Consultant—Type A	119
69 Consultant—Type B	120
70 Consultant—Type C	120
71 Consultants to User Agencies Employed Under Civil Service Procedures	121

SECTION VIII. PARENT-SUBSIDIARY AND MULTIPLE FACILITY ORGANIZATIONS

72 Parent-Subsidiary Relationship	123
73 Multiple Facility Organizations	124
74 Temporary Help Suppliers	125

SECTION IX. SENSITIVE COMPARTMENTED INFORMATION COMSEC INFORMATION

75 SENSITIVE COMPARTMENTED INFORMATION	127
76 COMSEC Information	127

SECTION X. GRAPHIC ARTS

77 Special Requirements for Graphic Arts	129
78 Production Control Records	129
79 Area Controls—Additional Requirements	129
80 Special Conditions	130
81 Destruction—Special Requirements	131
82 Mailing Lists	131

SECTION XI. NATO INFORMATION

83 Application	133
84 Authority	133

Paragraph	Page
85 Supervision and Orientation Requirements	133
86 Security Clearances	134
87 Reproduction, Preparation, and Marking	134
88 Transmission of NATO Material	134
89 Functions of the Contracting Officer	135
90 NATO Reporting Requirements	135
91 Subcontracting	135

SECTION XII. OVERSEAS OPERATIONS

Part 1. Access to U.S. Classified Information

92 General	137
93 Access to Classified Information	137
94 Safeguarding of U.S. Classified Information	138
95 Overseas Assistance	139
96 Notification of Overseas Assignment	139
97 Security Briefings and Certificates	140

Part 2. Access to Classified Information of Foreign Governments and International Pact Organizations Under A Security Assurance

98 General	141
99 Security Assurance	141

SECTION XIII. SECURITY REQUIREMENTS FOR ADP SYSTEMS

100 Applications and Purpose	143
101 Definitions	143
102 General	145
103 Personnel and Physical Controls	145
104 Clearance of Main Memory, Other Magnetic Media, and Equipment	147
105 Declassification Procedure	148
106 Dedicated Mode	149
107 Transmission	150
108 Subcontracting Classified Data Processing	151
109 Audit Trail	151
110 Multi-Level Resource-Sharing Systems	152

APPENDIX I. INDUSTRIAL SECURITY FORMS

Paragraph	Page
A. Application	153
B. Department of Defense Personnel Security Questionnaire (Industrial) (DD Form 48)	153
C. Application and Authorization for Access to Confidential Information (DD Form 48-2)	161
D. Department of Defense Personnel Security Questionnaire (Updating) (DD Form 48-3)	165
E. Department of Defense Personnel Security Questionnaire (Industrial) (Multiple Purpose) (DD Form 49)	169
F. Contract Security Classification Specification (DD Form 254)	177
G. Reserved	
H. Applicant Fingerprint Card (FD Form 258)	189
I. Request for Visit or Access Approval (ERDA Form 277)	193
J. Letter of Notification of Facility Security Clearance (DLA Form 381-R)	195
K. Letter of Notification of Security Assurance to a Foreign Government or International Pact Organization (DISCO Form 382)	197
L. Department of Defense Security Agreement (DD Form 441) and Appendage (DD Form 441-1)	199
M. Certificate Pertaining to Foreign Interests (DD Form 441s)	205
N. Security Briefing and Termination Statements (Industrial Personnel) (DLA Form 482)	209
O. Letter of Consent (DISCO Form 560)	211
P. Request for and Certificate of Cryptographic Access Authorization (DD Form 560-3)	213
Q. Personnel Security Clearance Change Notification (DLA Form 562-R)	215
R. Request for Administrative Termination of Personnel Security Clearance (DLA Form 683)	219
S. Envelope, Preaddressed to DISCO (DLA Form 703)	221
T. Envelope, Not Preaddressed (DLA Form 704)	221
U. Worksheet for the Preparation of Personnel Security Questionnaires, DD Forms 48 or 49 (DLA Form 707)	221
V. Facility Clearance Register (DD Form 1541) and Registration for Scientific and Technical Information Services (DD Form 1540)	227
W. Letter Agreement to Safeguard Classified Information for an Employee Performing Consultant Services	231

APPENDIX II. DOWNGRADING AND DECLASSIFICATION

A. Scope and Application	233
B. Automatic Downgrading and Declassification	235
C. Material Exempted From the GDS	236
D. Completion of CLASSIFIED BY, DECLASSIFY ON, and EXEMPTION CATEGORY Spaces	237
E. Electrically Transmitted Messages	237

Paragraph	Page
F. Re-marking Pre-June 1, 1972 Material	238
G. Marking New Material Prepared on or After June 1, 1972, Based on Pre-June 1, 1972 Source Material, or a Pre-June 1, 1972 Classification Guide Which Has Not Been Revised to Reflect E.O. 11652	238
H. Most Restrictive Marking Determination	239
I. Dates or Events Carried Forward	239
J. Changing Classification Markings	239
K. Re-Marking Pre-June 1, 1972 Material On Hand	239
L. Release of Declassified Information	239

APPENDIX III. FOREIGN CLASSIFIED CONTRACTS

Table Outlining Responsibilities for Security Actions	241
---	-----

APPENDIX IV. OUTLINE CONSTRUCTION SPECIFICATIONS FOR STORAGE VAULTS

A. Application	243
B. Class A Vault	243
C. Class B Vault	243
D. Class C Vault	244
E. Structural Design	244
F. Strongrooms	244

APPENDIX V. GUIDELINES FOR THE PHYSICAL CONSTRUCTION OF CLOSED AREAS

A. Application	247
B. Guidance	247

APPENDIX VI. EXTRACTS OF THE ESPIONAGE AND SABOTAGE ACTS AND OTHER FEDERAL CRIMINAL STATUTES	249
---	-----

APPENDIX VII. GUIDANCE FOR PREPARATION OF DEFENSIVE SECURITY BRIEFING

A. General	255
B. Introduction	255
C. Rationale	255
D. The Communist Country Intelligence Network	255
E. Techniques Employed to Obtain Information of Intelligence Value	255
F. Summary	257

APPENDIX VIII. INFORMATION REGARDING DCASRs, DISCO, DISI AND OISE	259
---	-----

APPENDIX IX. PUBLIC INFORMATION SECURITY GUIDANCE	265
---	-----

APPENDIX X. USE OF ESCORTS FOR CLASSIFIED SHIPMENTS

Paragraph	Page
A. General	269
B. Instructions and Operating Procedures	269
C. Functions of an Escort	269

APPENDIX XI. REQUIREMENTS APPLICABLE TO THE
HAND CARRYING OF CLASSIFIED DOCUMENTS
ABOARD COMMERCIAL PASSENGER AIRCRAFT

A. General	271
B. Approval	271
C. Authorization Letter and Identification Card	271
D. Preparation for Transmission - Packaging	272
E. Records	273
F. Briefings	273
G. Instructions to Traveler	273

SECTION I

GENERAL

1. Scope

a. This Manual establishes the requirements for safeguarding all classified information to which contractors and their subcontractors, vendors or suppliers have access or possession (see paragraph 3u). The Manual is written in terms of the most common situation where the contractor has access to, or possession of, classified information in connection with the performance of a classified contract. However, it also is applicable to the safeguarding of classified information in connection with all aspects of precontract activity, including preparation of bids and proposals and precontract negotiations, and all aspects of postcontract activity. Moreover, the requirements are equally applicable to the safeguarding of classified information not released or disclosed under a procurement contract such as classified information released pursuant to a User Agency program participated in by contractors on a voluntary or grant basis. Examples are: the long-range scientific and technical planning programs and programs designed to provide planning briefings for industry. In such situations the official of the User Agency (or his designated representative) who releases or discloses the classified information to the contractor shall fulfill the responsibilities which this Manual assigns to the contracting officer (e.g., furnishing necessary classification guidance, authorizing retention of classified material, certifying contractors' need to attend classified meetings).

b. The requirements of this Manual reflect the provisions of applicable Federal Statutes, E.O.s and DoD Directives.

c. The Secretary of Defense is authorized to act in behalf of the departments and agencies listed below in rendering industrial security services. This authority is contained in an exchange of letters between the Secretary of Defense and (i) The Administrator, NASA; (ii) The Secretary of Commerce; (iii) the Administrator, GSA; (iv) The Secretary of State; (v) The Administrator, Small Business Administration; (vi) The Director, National Science Foundation; (vii) The Secretary of the Treasury; (viii) The Secretary of Transportation; (ix) The Secretary of The Interior; (x) The Secretary of Agriculture; (xi) The Secretary of Health, Education and Welfare; (xii) The Secretary of Labor; (xiii) The Administrator, Environmental Protection Agency; (xiv) The Administrator, Federal Energy Administration; (xv) The Attorney General, Department of Justice, and (xvi) The Director, U.S. Arms Control and Disarmament Agency.

d. The ASD (C), his designee, or higher authority provides overall policy guidance for the Defense Industrial Security Program. The DLA-DD (CAS), shall administer the Defense Industrial Security Program on behalf of all User Agencies. Except for certain functions performed by the Commander or Head of a User Agency installation with respect to those facilities or contractor activities located on the installation, the Commander of each DCASR shall perform cognizant security office functions prescribed in this Manual with respect to all contractor facilities within his region. (See Appendix VIII for geographical areas of responsibility.)

e. User Agencies have the authority of, and exercise the functions of, a contracting officer as prescribed in this Manual and the ISR. Certain of these functions are, under the delegation of contract administration services, performed by the DLA-DD(CAS). In addition, other contracting officer duties may be performed by the ACO, DCASR, within the contract administration services delegation.

f. This Manual also shall apply to the safeguarding of foreign classified information which has been furnished to U.S. contractors and which the U.S. Government is obligated to protect in the interest of national defense. When foreign classified information is made available to a contractor by a User Agency in connection with a U.S. classified contract, procedures applicable to U.S. classified information shall apply. However, when foreign classified information is made available to U.S. contractors in connection with a foreign classified contract, the responsibility for the actions which this Manual charges to the contracting officer and the contracting User Agency shall be as prescribed in Appendix III. Responsibilities not specifically assigned in Appendix III are reserved to the foreign government agency or foreign contracting activity concerned.

g. Revisions to this Manual which have been approved by the DASD (SP) will be published in page change form and will be effective the date of the change.

2. Applicable Federal Statutes, Executive Orders and Regulations

a. Espionage Acts, Title 18, U.S.C., Sections 793 through 799.

b. Sabotage Acts, Title 18, U.S.C., Sections 2151 through 2157.

c. Conspiracy Statute, Title 18, U.S.C., Section 371.

d. Internal Security Act of 1950 (in part), Title 50, U.S.C., Sections 781 through 798.

e. National Security Act of 1947, as amended.

f. Armed Services Procurement Act of 1947, as amended.

g. Atomic Energy Act of 1954, Public Law 703, 83d Congress, as amended.

h. E.O. 10104, 1 February 1950.

i. E.O. 11652, 8 March 1972.

j. National Aeronautics and Space Act of 1958, as amended.

k. E.O. 10865, 20 February 1960.

l. Federal Aviation Act of 1958, as amended.

m. E.O. 10909, 17 January 1961.

n. International Traffic in Arms Regulation, Code of Federal Regulations, Title 22, Chapter 1, Parts 121-127.

o. Export Control Act of 1949, as amended.

p. Mutual Security Act of 1954, as amended.

3. Definitions

The following definitions are established for the purpose of this Manual:

a. *Access, Accessibility.* The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures which are in force do

not prevent him from gaining knowledge of the classified information.¹

b. Alien. Any person not a citizen or national of the U.S. (see Immigrant Alien, paragraph 3aj).

c. Authorized Persons. Those persons who have a need-to-know for the classified information involved, and have been cleared for the receipt of such information (see paragraph 3as). Responsibility for determining whether a person's duties require that he possess, or have access to, any classified information and whether he is authorized to receive it, rests upon the individual who has possession, knowledge, or control of the information involved, and not upon the prospective recipient.

d. Candidate Material. That material which is referred to collectively as special nuclear materials and nuclear weapons.

e. Carrier Custodian. An employee of a cleared carrier who has been assigned the responsibility for SECRET controlled shipments by the carrier and who has been issued a personnel security clearance by the Government.

f. Classified Contract. Any contract that requires or will require access to classified information by the contractor or his employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.)

g. Classified Information. Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure, and which has been so designated.

¹ The entry into a controlled area, per se, will not constitute access to classified information if the security measures which are in force prevent the gaining of knowledge of the classified information. Therefore the entry into a controlled area under conditions that prevent the gaining of knowledge of classified information will not necessitate a personnel security clearance.

h. Closed Area. A controlled area established to safeguard classified material, which, because of its size or nature, cannot be adequately protected by the safeguards prescribed in paragraph 16 or be stored during nonworking hours in accordance with paragraph 14 (see Section IV).

i. Closed Vehicle. A conveyance which is fully enclosed by sides, permanent top and door.

j. Cognizant Security Office. The DCASR having contract administration services jurisdiction over the geographical area in which a facility is located.

k. Colleges and Universities. All educational institutions which award academic degrees and their related research activities directly associated therewith through organization or by articles of incorporation.

l. Reserved.

m. Communications Intelligence. Technical and intelligence information derived from foreign communications by other than the intended recipient.

n. COMMUNICATIONS SECURITY (COMSEC). The protection resulting from the application of cryptosecurity, transmission security, and emission security measures to communications and from the application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value which might be derived from the possession and study of such communications, or to insure the authenticity of such communications.

o. Compromise. The known or suspected exposure of classified information or material to an unauthorized person.

p. CONFIDENTIAL. CONFIDENTIAL refers to that national security information

or material, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

q. Consignee. A person, firm or Government activity named as the receiver of a shipment; one to whom a shipment is consigned.

r. Consignor. A person, firm or Government activity by whom articles are shipped. The consignor is usually the shipper.

s. Continental Limits of the United States. U.S. territory including the adjacent territorial waters located within the North American continent between Canada and Mexico.

t. Contracting Officer. Any person who, in accordance with departmental or agency procedures, is currently designated a contracting officer with the authority to enter into and administer contracts and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his authority. For purposes of this Manual, the term contracting officer refers to the contracting officer at the purchasing office who is identified as the PCO and the contracting officer at a contract administration office who is identified as the ACO. Normally, the responsibilities which this Manual assigns to the contracting officer during the precontract, contract award and post contract stages of a classified procurement will be performed by the PCO, with the ACO performing those responsibilities which arise during the performance stages of a classified contract.

u. Contractor. Any industrial, educational, commercial, or other entity which has executed a contract with a User Agency or a DoD Security Agreement (DD Form 441) with a DoD agency or activity.

v. CRYPTO. A designation or marking which identifies classified operational key-

ing material, and which indicates that this material requires special consideration with respect to access, storage and handling.

w. Declassify. To cancel the security classification of an item of classified material.

x. Department of Defense. Office of the Secretary of Defense (including all boards, councils, staffs and commands), DoD agencies, and the Departments of the Army, Navy, and Air Force (including all their activities).

y. Document. Any recorded information, regardless of its physical form or characteristics, exclusive of machinery, apparatus, equipment or other items of material. The term includes, but is not limited to the following all written material, whether handwritten, printed or typed; all photographs, negatives, exposed or printed films, and still or motion pictures; all data processing cards or tapes; maps; charts; paintings; drawings; engravings; sketches; working notes and papers; and all reproduction of the foregoing by whatever process reproduced; and sound, voice and electronic recordings in any form.

z. Downgrade. To assign a lower security classification to an item of classified material.

aa. Executive Personnel. Those individuals in managerial positions, other than owners, officers, or directors, who administer the operations of the facility. (This category includes such designations as general manager, plant manager, plant superintendent, or similar designations, and facility security supervisor.)

ab. Facility. A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities and components, which, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined above.) For purposes

of industrial security, the term does not include User Agency installations.

ac. Facility Security Clearance. An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

ad. Foreign Classified Information. Official information of a foreign government which: it has classified; the U.S. Government has determined requires protection in the interest of national security; has been furnished to a U.S. contractor in connection with a contract, subcontract, precontract negotiation or other arrangement approved by the U.S. Government; and the U.S. Government is obligated to protect pursuant to an agreement with that government.

ad. 1. Foreign Interest. Any foreign government or agency of a foreign government; any form of business enterprise organized under the laws of any country other than the U.S., or its possessions; any form of business enterprise organized or incorporated under the laws of the U.S., or a State or other jurisdiction of the U.S. which is owned or controlled by a foreign government, firm, corporation or person. Included in this definition is any natural person who is not a citizen or national of the U.S. (An "immigrant alien" as defined in paragraph 3aj is excluded from the definition of a foreign interest.)

ae. Foreign Nationals. All persons not citizens of, not nationals of, nor immigrant aliens to, the U.S.

af. FORMERLY RESTRICTED DATA. Information which has been removed from the RESTRICTED DATA category by joint action of the ERDA and DoD under Section 142d, Atomic Energy Act of 1954, as amended. This action is based upon a determination by these agencies that the information relates primarily to the military utilization of atomic weapons, and that the

information can be adequately safeguarded as national security information. FORMERLY RESTRICTED DATA may not be transmitted or otherwise made available to any regional defense organization or foreign nation while it remains national security information except under the provisions of that Act.

ag. Graphic Arts. Facilities and individuals engaged in performing consultation, service, or the production of any component or end product which contributes to, or results in, the reproduction of classified information. Regardless of trade names of specialized processes, it includes writing, illustrating, advertising services, copy preparation, all methods of printing, finishing services, duplicating, photocopying, and film processing activities.

ah. Hardened Container. A container of such strength and durability as to provide security protection to prevent items from breaking out of the container and to facilitate the detection of any tampering with the container while in transit. Some examples of hardened containers are banded or wired boxes, wooden boxes and closed cargo transporters.

ai. Home Office. The headquarters facility of a multiple facility organization (see paragraph ap., below).

aj. Immigrant Alien. Any person lawfully admitted into the U.S. under an immigration visa for permanent residence. (See paragraph 25 for special prerequisites for clearance of immigrant aliens.)

ak. Industrial Security. That portion of internal security which is concerned with the protection of classified information in the hands of U.S. industry.

al. Information. Knowledge which can be communicated by any means.

am. Intelligence. The product resulting from the collection, evaluation, analysis, in-

tegration and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of foreign operations, and which is immediately or potentially significant to military planning and operations.

an. Locked Entrance. A locked entrance is an entrance to a Closed or Restricted Area which is kept closed and locked at all times except when temporarily unlocked and opened under supervision for the purpose of passing material or authorized personnel into or out of the area.

ao. Material. Any document, product or substance on, or in which, information may be recorded or embodied. Material shall include everything, regardless of its physical character or makeup. Machinery, documents, apparatus, devices, models, photographs, recordings, reproductions, notes, sketches, maps, and letters, as well as all other products, substances or materials, shall fall within the general term of material.

ap. Multiple Facility Organization. A legal entity (single proprietorship, partnership, association, trust, or corporation) which is composed of two or more facilities (see paragraph *ab.*, above).

aq. National of the United States.

- (1) A citizen of the U.S., or—
- (2) A person who, though not a citizen of the U.S., owes permanent allegiance to the U.S.²

ar. NATO Classified Information. The term "NATO classified information" embraces all classified information, military, political, and economic, circulated within and by NATO whether such information

originates in the organization itself or is received from member nations or from other international organizations.

as. Need-to-Know. A determination made by the possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to (see paragraph *a.*, above), knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by a User Agency.

at. Negotiator. Any employee, in addition to the OODEPs, who requires access to classified information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime or subcontract. (This category may include, but is not limited to, accountants, stenographers, clerks, engineers, draftsmen, and production personnel.)

at.1 Nuclear Weapon Security Program. A limited number of defense contractors are involved in the DoD nuclear weapon security program. This program identifies certain positions categorized as Critical or Controlled, depending upon the degree of involvement with nuclear weapons. Assignment to such positions is governed by the DoD Nuclear Weapon PRP, the specific procedures of which will be set forth separately in appropriate contractual agreements. All personnel in Critical or Controlled positions must have a security clearance commensurate with the security classification of information required by their duties.

au. Officers (Corporation, Association, or Other Type of Business or Educational Institution). Those persons in positions established as officers in the articles of incorporation or bylaws of the organization.

av. Official Information. Information which is owned by, produced for or by, or is subject to the control of the U.S. Government.

² See 8 U.S.C. Sec. 1101(a) (22). 8 U.S.C. Sec. 1401, subsection (a) lists in paragraphs (1) through (7) categories of persons born in and outside the U.S. or its possessions who may qualify as nationals of the U.S. Where doubt exists as to whether or not a person can qualify as a national of the U.S., this subsection should be consulted.

aw. Possessions. Possessions include the Virgin Islands, Guam, American Samoa, the Guano Islands with Swains Island, Howland Island, Baker Island, Jarvis Island, Midway Islands, Kingman Reef, Johnson Islands, Sand Island, Navassa Island, Swan Islands and Wake Island.

aw.1 Principal Management Facility. A cleared facility of a multiple facility organization which reports directly to the home office, and whose principal management official has been delegated the responsibility to administer the contractor's industrial security program, within a defined geographical or functional area.

ax. Protective Security Service. A signature security service, as described in paragraph *bk.*, below, plus constant protection of the shipment at all times between receipt from the consignor until delivery to consignee, by one or more carrier custodians. In the case of air movement, however, observation of the shipment is not required during the period it is stored in the carrier's aircraft in connection with flight, provided the shipment is loaded into a compartment which is not accessible to any unauthorized person aboard. Conversely, if the shipment is loaded into a compartment of the aircraft which is accessible to an unauthorized person aboard, the shipment must remain under the constant surveillance of an escort or carrier custodian.

ay Qualified Carrier. A carrier which has met all of the following criteria:

- (1) The requirement for the carrier's service has been established by a shipper.
- (2) The carrier is authorized by law, regulatory body or regulation to provide the required transportation service.
- (3) A determination has been made by MTMC or the designated Commander overseas that (i) the carrier is capable of and authorized to furnish Protective Security Service in accordance with an applicable tariff, Gov-

ernment tender, agreement or contract provision, and (ii) no other qualified carrier is available to perform the required service.

- (4) The carrier has executed a DoD Transportation Security Agreement (DLA Form 1149) with, and has been granted a SECRET facility security clearance by the appropriate cognizant security office.

az. Reference Material. The term reference material means documentary material over which the User Agency does not have classification jurisdiction, and did not have classification jurisdiction at the time such material was originated.

ba. Regrade. To assign a higher or lower security classification to an item of classified material.

bb. Representatives of a Foreign Interest. Citizens or nationals of the U.S. or immigrant aliens who, in their individual capacity, or on behalf of a corporation (whether as a corporate officer or official or as a corporate employee who is personally involved with the foreign entity), are acting as representatives, officials, agents, or employees of a foreign government, firm, corporation, or person. However, a U.S. citizen or national who has been appointed by his U.S. employer to be its representative in the management of a foreign subsidiary (i.e., a foreign firm in which the U.S. firm has ownership of at least 51% of the voting stock) will not be considered a representative of a foreign interest, solely because of this employment, provided the appointing employer is his principal employer and is a firm that possesses or is in process for a facility security clearance.

bc. Restricted Area. A controlled area established to safeguard classified material which, because of its size or nature, cannot be adequately protected during working hours by the safeguards prescribed in para-

graph 16, but which is capable of being stored during non-working hours in accordance with paragraph 14 (see Section IV).

bd. RESTRICTED DATA. All data (information) concerning (i) design, manufacture or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but not to include data declassified or removed from the RESTRICTED DATA category pursuant to Section 142 of the Atomic Energy Act (see Section 11y, Atomic Energy Act of 1954, as amended, and FORMERLY RESTRICTED DATA).

be. SECRET. SECRET refers to that national security information or material, the unauthorized disclosure of which could reasonably be expected to cause *serious damage* to the national security.

bf. SECRET Controlled Shipment. SECRET material moving in commercial transportation service which requires Protective Security Service of a qualified carrier in the interest of national security.

bg. Security. Refers to the safeguarding of information classified TOP SECRET, SECRET, or CONFIDENTIAL against unlawful or unauthorized dissemination, duplication, or observation.

bh. Security Cognizance. The responsibility for acting for User Agencies in the discharge of industrial security responsibilities described in this Manual.

→ *bh.1. SENSITIVE COMPARTMENTED INFORMATION.* This term includes all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include RESTRICTED DATA as defined in

Section II, Public Laws 585, Atomic Energy Act of 1954, as amended.

bi. Shipper. The one who releases custody of material to a carrier for transportation to a consignee (see also *consignor*, paragraph r.).

bj. Short Title. An identifying combination of letters and numbers assigned to a publication or equipment for purposes of brevity.

bk. Signature Security Service. A service designed to provide continuous responsibility for the custody of shipments in transit, so named because a signature and tally are required from each person handling the shipment at each stage of its transit from point of origin to destination. For air shipments no receipt is required from the flight crew or attendants of the carrier's aircraft. For rail shipments no receipt is required from the train crew if the car is sealed.

bl. Single Line Service. Freight which moves from point of origin to destination over the lines of only one carrier.

bm. Special Access Program. Any program imposing "need-to-know" or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET or TOP SECRET information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements, material dissemination restrictions or special lists of persons determined to have a "need-to-know."

bn. Subsidiary. A subsidiary is a corporation which is controlled by another corporation (parent) by reason of the latter corporation's ownership of at least a majority (over 50%) of the capital stock. A subsidiary is a legal entity and shall be processed separately for a facility security clearance.

bo. Reserved.

bp. TOP SECRET. TOP SECRET refers to that national security information or material, the unauthorized disclosure of which could reasonably be expected to cause *exceptionally grave damage* to the national security.

bq. Transshipping Activity (Government). A Government activity to which a carrier transfers custody of freight for reshipment by another carrier to the consignee.

br. Trust Territory. Applies only to the Trust Territory of the Pacific Islands which the United States administers under the terms of a trusteeship agreement concluded between this Government and the Security Council of the United Nations pursuant to authority granted by Joint Resolution of Congress, July 18, 1948 (61 Stat. 397; 48 U.S.C., Section 1681). According to this agreement, the U.S. has "full powers of administration legislation, and jurisdiction" over the territory; this Government, however, does not claim "sovereignty." Three major archipelagoes make up the Trust Territory: Carolines (including the Palau Islands), Marshalls, and Marianas (excluding Guam).

bs. Unauthorized Person. Any person not authorized to have access to specific classified information in accordance with the provisions of this Manual.

bt. United States. The 50 States and the District of Columbia.

bu. Upgrade. To determine that certain classified information requires, in the interests of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect the higher category.

bv. User Agencies. The OSD (including all boards, councils, staffs and commands), DoD agencies and Departments of the Army, Navy and Air Force (including all of their activities); Departments of: State; Commerce; Treasury; Transportation; Interior; Agriculture; Health, Education and Welfare; Labor and Justice; NASA; GSA; SBA; NSF; EPA; FEA, and ACDA.

bw. Weapon System. A general term used to describe a weapon and those components required for its operation.

4. Designation of Cognizant Security Office

Responsibility for administration of the Defense Industrial Security Program is assigned to the DLA-DD(CAS). The authority for security cognizance has been delegated to the Commanders, DCASRs for all contractor facilities physically located or to be located within the geographic boundaries of each Region (see Appendix VIII). All relationships between the User Agency and the contractor on industrial security matters shall be handled through, or in coordination with, the cognizant security office, except those matters specifically set forth in this Manual as responsibilities of the contracting officer. All questions of interpretation with respect to this Manual, or problems involving the industrial security procedures as they pertain to the contractor, shall be forwarded to the cognizant security office. In the case of a facility or contractor activity located on a User Agency installation, requests for interpretations of this Manual shall be forwarded to the cognizant security office through the Commander or Head of the User Agency installation. The management of each facility which has been assigned to one of the DCASR offices for security cognizance shall be notified in writing of this action at such time as the Industrial Security Program is initiated at the facility. The designation of a DCASR to exercise security cognizance at a facility will not relieve any User Agency of the responsibility for protecting and safeguarding its classified information incident to its classified contracts with the facility, or from visiting the facility to review the security aspects of such contracts. However, the security administration of a U.S. classified contract awarded to a U.S. contractor which requires performance for a User Agency at a location outside the U.S., Puerto Rico, Panama Canal Zone, or a U.S. possession, territory or trust territory shall be the responsibility of the User Agency awarding the classified contract except when the contracting User Agency has an agreement with the U.S. Installation Commander in such

area to perform this function for it. The DCASR Commander for the region in which the home office or principal U.S. based office of the contractor is located will assume security cognizance for such U.S. based facility, and except for contractor granted CONFIDENTIAL clearances, DISCO will clear all of the contractor's employees requiring access to classified information in support of a User Agency contract regardless of the physical location of such employees. Contractor activities located outside the U.S., Puerto Rico, Panama Canal Zone or a U.S. possession, territory or trust territory will not be granted a facility clearance.

5. General Requirements

The contractor shall be responsible for safeguarding all classified information under his control. In the furtherance of this requirement, the contractor—

a. Security Supervisor. Shall appoint a U.S. citizen, who is required to be cleared as part of the facility security clearance, to supervise and direct security measures necessary for the proper application of Government furnished guidance or specifications for classification, downgrading, upgrading, and for safeguarding classified information.

b. Automatic Data Processing. Shall not utilize an ADP system for the processing of classified data without the prior approval of the cognizant security office (see Section XIII).

c. Limitation on Disclosure. Shall assure that classified information is furnished or disclosed only to authorized persons (see paragraph 3c). To this end he shall determine to what extent his employees, subcontractors, vendors, and suppliers require access to classified information in the performance of tasks or services essential to the ful-

fillment of the contract.³ He shall take all reasonable measures to adjust plant layout and organize work so as to limit such access to the least number of individuals or firms consistent with the efficient performance of the classified contract. In those exceptional cases where the contractor cannot adjust plant layout and organize work so as to prevent access by representatives of food, beverage, or vending equipment organizations, he may request his cognizant security office to process the servicing organization for a facility security clearance provided the management of the facility can justify the continued need for the service. Representatives of cleared service organizations shall, in such cases, be processed as Category 1 visitors at the facility being visited (see paragraph 41a).

d. Safeguarding. Shall provide suitable protective measures within his facility for the safeguarding of classified information. A contractor performing work within the confines of a User Agency installation must safeguard classified information in accordance with provisions of this Manual, unless responsibilities for security are modified by the contract. All classified material received by the contractor which:

- (1) is not related to a contract, project or program pursuant to paragraph 1a; and
- (2) for which no safeguarding or disposition instructions have been received, shall be safeguarded in accordance with the provisions of this Manual and the cognizant security office shall

³ A contractor is not authorized to turn over classified intelligence information to a subcontractor, vendor or supplier without prior written authorization of the contracting User Agency. All classified intelligence information, whether obtained during a visit or through other sources, shall be safeguarded and controlled in accordance with the provisions of this Manual, and any additional instructions which may be received from the releasing User Agency activity and any specific restrictive markings or limitations appearing on documents. All inquiries concerning source, acquisition, use, control or restrictions pertaining to intelligence information shall be directed to the contracting User Agency activity concerned.

be notified pursuant to paragraph 6a(19).

e. Exclusion of Personnel. Shall exclude from those parts of his plants, facilities, or sites where classified work is being performed, any person or persons whom the Head of a User Agency concerned or his authorized representative, in the interest of security, may designate in writing. Exclusion does not mean that the affected employee must be dismissed or be denied employment in another part of the plant, facility, or site. This should be resolved consistent with normal employer-employee relationships.

f. Individual Responsibility for Safeguarding. Shall, on a recurring basis, bring to the attention of his personnel, engaged in the preparation of bids, quotations, or in the performance of work on contracts or programs which involve access to classified information, their continuing individual responsibilities for safeguarding classified information. Each employee shall be made aware of the security procedures which pertain to his particular work assignment and of any security deficiencies resulting from recurring inspections by the cognizant security office that required individual corrective action on his part. The employee who has possession or knowledge of an element or item of classified information shall be informed that he is responsible for determining whether a prospective recipient is an authorized person (see paragraph 3c). The employee shall be informed that he is required to advise the recipient of the classification of the information which he discloses. The contractor shall also inform his employees that unauthorized disclosure of classified information violates DoD regulations and contractual obligations, and is punishable under the provisions of Federal criminal statutes.

g. Security Briefing and Termination. Shall, prior to permitting an employee to have access to classified information, brief

him on his obligation to safeguard classified information, advise him of its importance, inform him of the required security procedure and have him read, or have read to him, the portions of the espionage laws, conspiracy laws, and Federal criminal statutes applicable to the safeguarding of classified information appearing in Appendix VI of this Manual. In addition, the employee shall be advised that he must report to the contractor if he becomes a representative of a foreign interest (see paragraph 3bb). Following the briefing the employee shall be required to execute Part I of Security Briefing and Termination Statements (DLA Form 482). The DLA Form 482 shall then be retained by the contractor. An employee who executes Part I of DLA Form 482 and who subsequently is absent from his place of employment, for any reason, in excess of 12 months, must re-execute Part I of DLA Form 482 before again being permitted access to classified information. The employee shall be required to execute Part II of DLA Form 482 at the time of termination of employment (discharge, resignation or retirement) and at the beginning of a layoff or leave of absence for an indefinite period or for a period in excess of 12 months; upon termination or revocation of the facility's security clearance; or when administrative termination of personnel security clearance is accomplished in accordance with the provisions of paragraph 29. The contractor shall retain Part II, DLA Form 482, or its predecessor form, for not less than 3 years where an employee has had access to TOP SECRET or other information requiring a special access to TOP SECRET or other information requiring a special access authorization by the Government, and for not less than 2 years where an employee has had access to SECRET or CONFIDENTIAL information. The importance of the termination statement shall be brought to the terminating employee's attention. If the terminating employee had access to TOP SECRET, COMSEC, or other information requiring a special access authorization by the Government, he shall be given an oral debrief-

ing which shall include a statement of (i) the purpose of the debriefing; (ii) the serious nature of the subject matter which requires protection in the national interest; (iii) the need for caution and discretion; and (iv) advice concerning any travel restrictions which are appropriate. The cognizant security office shall be notified immediately in accordance with paragraph 6a(9) of the circumstances involved whenever an employee refuses to execute the DLA Form 482.⁴

h. Special Features of Design. Shall not incorporate any special features of design or construction in any project other than that for which they are furnished by, developed for, or designed for the Government, if such incorporation would disclose classified information unless prior written authorization of the contracting officer concerned has been obtained. However, classified features of design or construction may be incorporated by the contractor in other U.S. User Agency projects of equal or higher classification unless specifically prohibited by the Government. U.S. classified information shall not be used in the performance of a foreign classified contract unless the information was furnished through the designated military department in connection with that contract, or the U.S. contracting officer concerned has expressly authorized in writing the use of that information.

i. Security of Combinations. Shall insure

⁴ When a terminated employee fails to execute Part II of DLA Form 482, the contractor shall make every reasonable effort to contact the former employee for the purpose of correcting the omission—for example, enclosing a copy of the form in a registered or certified letter, return receipt requested, sent to the former employee's last known address. If, once contact is established with the former employee, he fails to comply with the request to execute and return the form, such failure shall be considered as tantamount to a refusal and should be reported as such in accordance with paragraph 6a(9). Conversely, if despite such efforts contact cannot be established with the former employee, a report should also be submitted under paragraph 6a(9), indicating what efforts had been made to locate the former employee. Where the employee was also required to be given an oral debriefing, the contractor may, if the former employee is located at a remote distance from the facility, direct him to contact the nearest cognizant security office and make arrangements to receive the required debriefing. In such case, the cognizant security office should be requested in writing to perform the debriefing on behalf of the contractor.

that the combinations to safes, containers, and three-position, dial-type changeable combination padlocks used to lock containers holding classified material are classified in accordance with the classification of the highest classified material stored in the containers. The combinations shall be changed at intervals of at least once every year (if NATO or CRYPTO classified material is stored, the combination shall be changed every six months) and at the earliest practicable time following—

- (1) The reassignment, transfer or discharge of any person having knowledge of the combination, or when the security clearance granted to any such person is downgraded to a level lower than the category of material stored, or is suspended or revoked by proper authority.
- (2) The compromise or suspected compromise of the safes and containers or their combinations, or discovery of the container being left unlocked and unattended.
- (3) The initial receipt of safes, containers, and three-position, dial-type, changeable combination padlocks.

Combinations to safes, containers and three-position, dial-type changeable combination padlocks shall be changed under the above schedule by a person entrusted with the combination or authorized access to the contents of the container in accordance with paragraph 14c, or by the facility security supervisor or his designated representative. Under no circumstances shall the changing of the combinations be performed by an outside locksmith or subcontractor employee. To prevent unauthorized substitution, combination padlocks shall be either placed inside of the open container or secured to a hasp, drawer or handle of the container when it is open.

j. Security Checks. Shall perform security checks within the facility to insure that at all times security precautions are taken to

protect classified material in the possession of the facility and shall designate an individual or individuals to make room or area checks during normal working hours to insure that all classified material not under surveillance has been properly stored.

k. Transmission. Shall establish procedures for the proper transmittal of classified material in accordance with the provisions of paragraph 17.

l. Disposition of Classified Material. Shall return to the contracting officer, or his designated representative all classified material furnished by a User Agency, including all reproductions thereof, and shall surrender all classified material developed by the contractor in connection with a User Agency contract, program or proposal^{5 6} unless the material has been destroyed in accordance with paragraph 19, or the retention of the material is authorized under the provisions of paragraph *m*, below. Such material shall be returned or surrendered in accordance with the following schedule:

(1) *If a bid, proposal or quote is not submitted or is withdrawn.* Within 90 days after the opening date of bids, proposals or quotes.

(2) *If a bid, proposal or quote is not accepted.* Within 90 days after notification that a bid, proposal or quote has not been accepted. If further retention is necessary to serve a User Agency purpose, a request for approval shall be submitted to the appropriate contracting officer in accordance with paragraph *m*, below.

⁵ The placing of an appropriate notation on each document indicating the specific contract to which it pertains will assist in achieving compliance with this paragraph.

⁶ Classified material of the type described in the next to the last sentence of paragraph 1a, which is not related to a proposal or classified contract, may be destroyed in accordance with the provisions of paragraph 19c (unless specifically prohibited), or disposed of in accordance with such instructions as may be issued by the User Agency which originally furnished such material.

(3) *If a successful bidder.* Upon final delivery of goods or services, or upon complete termination of the contract, unless otherwise prescribed in the contract or directed by the contracting officer.

m. Retention of Classified Material.

(1) May retain classified material in special cases when a bid, proposal or quote is not accepted or upon completion or termination of the contract provided the contractor requests and justifies such retention and its retention is agreed to by the contracting officer. The contractor shall be authorized to retain classified material only—

(a) When retention is necessary for the maintenance of the contractor's essential records; or

(b) When classified information is also patentable or is proprietary data in which the contractor has title; or

(c) When retention of the material will assist the contractor and will benefit the Government in the performance of other User Agency contracts (the contracting officer of a current classified contract may authorize transfer of the material to the current contract when the material is identified by the contractor in accordance with the procedure set forth in paragraph 5m(4)⁷. In these situa-

⁷ When such approval is granted the contracting officer who had cognizance over the classified material shall be notified by the current contracting officer. In the event retention of information under the circumstances contemplated in this paragraph involves information of a DoD User Agency being retained by a contractor of a non-DoD User Agency, or vice versa, or between non-DoD agencies, the concurrence of the contracting officer of the completed or terminated contract or bid which was not accepted must be obtained by the current contracting officer prior to the authorization for retention being granted. Information authorized for retention under these circumstances will be identified as to its origin, and its ultimate disposition or declassification will remain with its originating agency.

CH 1

DoD 5220.22-M

tions the material will be disposed of in accordance with paragraph 5l at the completion of the current contract.); and

- (d) When the contractor justifies and requests retention authority in writing, indicates the period of time retention is necessary and identifies the classified material for which retention is requested as follows: TOP SECRET and SECRET material shall be identified in a list of specific documents unless, in the case of SECRET material only, the contracting officer has authorized identification by subject matter and approximate number of documents; CONFIDENTIAL material shall be identified by subject matter and approximate number of documents. However, authorization of the contracting officer is not required for the retention of (i) records held by the contractor in accordance with the records retention requirements of the basic contract; (ii) records authorized for retention for a specific period under the terms of the basic contract; and (iii) records which, during the contract period, the contracting officer has authorized the contractor to retain for a specific period following completion of the contract, provided that, in each case, the contractor informs the contracting officer of the material to be retained, identifying it in the manner prescribed above.

- (2) Unless otherwise indicated on the material, may retain classified material which does not relate to a contract, e.g., obtained at classified

symposiums or meetings, only as long as needed, but not for a period to exceed one year from the date of receipt. Retention beyond that time is authorized only when the contractor requests and justifies such retention, and retention is agreed to by a contracting officer of a current contract or an official of the User Agency which released the information.

n. Termination of Security Agreement. Shall, notwithstanding the provisions of paragraphs l, and m, above, in the event that the Security Agreement is terminated for any reason by either party and is not superseded by a new Security Agreement, tender all classified material in his possession to the User Agency concerned, or dispose of such material in accordance with instructions from the User Agency concerned. The Letter of Notification of Facility Security Clearance (DLA Form 381-R) and the contractor's copy of the DoD Security Agreement (DD Form 441) shall be returned to the cognizant security office. Control station records, reproduction records, destruction certificates and visitor records for which the retention period is not expired at the time of termination of the Security Agreement shall continue to be maintained by the contractor until the expiration of the prescribed retention period. These records shall be subject to review and recall by the Government at any time within the retention period.

o. Public Release. Shall not release for public dissemination information pertaining to classified contracts or projects, except as provided in Public Information Security Guidance No. 16 (see Appendix IX), without the approval of the Directorate for Security Review, OASD(PA),⁸ in order to preclude the release of information requiring protection in the interest of national

⁸ If the information pertains to a classified contract or project awarded by a non-DoD agency, request for release shall be submitted to the contracting agency.

security within the meaning of E.O. 11652. Requests for release shall be submitted to the activity specified in item 13 of the Contract Security Classification Specification (DD Form 254). All information developed subsequent to the initial approval shall also be approved by the Directorate for Security Review prior to release. The provisions of this paragraph also apply to unclassified brochures, promotional sales literature, reports to stockholders or similar type material.⁹ As an exception to these release requirements, the authority to authorize the release of certain unclassified information pertaining to scientific results of research, development, test and evaluation, has been delegated to User Agencies.

p. Classified Sales Literature. Shall not publish or distribute, or permit to be published or distributed, brochures, promotional sales literature, or similar-type material containing classified information, without prior review and written authorization by the contracting officer concerned, or his designated representative. The authorization for such publication and distribution shall be indicated on the cover of the document or the first page of the document if there is no cover. However, publication and distribution to authorized persons (see paragraph 3c) may be made without specific authorization from the contracting officer for—

- (1) Classified material which is published or distributed for necessary use within the organization of the contractor or his subcontractor in the performance of the contract.
- (2) Classified material prepared in reply to a request for proposal or invitation to bid received from a User Agency or a cleared prime or subcontractor of a User Agency or classified information contained in

⁹ In addition to the requirements of this paragraph, the release of unclassified technical data is also governed by the Export Control Act of 1949, administered by the Secretary of Commerce, and Section 414 of the Mutual Security Act of 1954, as amended, administered by the Secretary of State through the ITAR.

an unsolicited proposal submitted to User Agency.

- (3) Classified material submitted in response to an official request of a User Agency.

q. Disclosure at Meetings. Shall not disclose in any manner classified information at a conference, seminar, symposium, exhibit, convention, or other gathering (hereinafter referred to as a meeting), except under the conditions described below:

- (1) At a meeting conducted pursuant to and as a necessary element of a specific contract held only in the prime or subcontractor's facility, and attended only by authorized persons who have a need-to-know in connection with the contract including employees of the contractor or subcontractors and consultants thereto, and authorized visitors; and over which meeting controls have been established to insure that the meeting site is physically secure, that the classified notes, minutes and summaries resulting from the meeting are properly safeguarded and that the attendees are given sufficient classification guidance during the oral presentations; or
- (2) At a meeting conducted by a DoD activity, provided that, when the information to be disclosed is under the jurisdiction of another Government agency or when the meeting is to be attended by representatives outside the DoD the contractor requests the conducting activity to obtain written approval from the contracting officer concerned prior to the disclosure. A copy of such request shall be furnished to the contracting officer concerned. The contractor is not required to obtain approval if only DoD information is to be disclosed, and only the

contractor, subcontractors, their employees, and DoD personnel are to attend the meeting; or

- (3) At a meeting conducted by a contractor, association, society, or group, and sponsored by the DoD (including the departments and agencies named in paragraph 1c), provided written approval of the contracting officer concerned is furnished to the sponsoring activity prior to the disclosure, and the additional requirements of paragraph 9 are fulfilled; or
- (4) At a meeting conducted or sponsored by Government agencies other than those referred to in paragraph (3) above, provided the contractor requests and obtains written approval from the contracting officer concerned prior to the disclosure.

r. Controlled Areas. Shall place in effect a system to control access of employees and visitors to Closed and Restricted Areas (see Section IV).

s. Standard Practice Procedure. Shall, prior to the issuance of a facility security clearance by the cognizant security office, submit a written SPP (interim or final) in sufficient detail to place into effect all security controls required by the DD Form 441 and this Manual which are applicable to the operations of the facility. An interim SPP must implement requirements of this Manual which are immediately applicable to the operations of the facility in connection with the facility's anticipated involvement in the Defense Industrial Security Program. A multiple facility organization or, as provided for in paragraph 72c, a parent-subsidiary organization may publish an SPP applicable throughout the organization, but such publication shall then be adapted as necessary to apply at specific operating locations. A copy of the SPP shall be furnished to

each appropriate cognizant security office. The contractor shall modify the SPP upon notification from the cognizant security office that it does not adequately implement the requirements of this Manual. The SPP may be revised at any time after promulgation of a revision to this Manual. However, the SPP shall be revised, as necessary, to implement the revisions applicable to the contractor's operation within 4 months after a revision has been incorporated in reprinted pages of this Manual. The SPP for a facility at which only one employee or management official is assigned shall provide for the notification to the cognizant security office of the death or incapacitation of that employee. Specifically, the SPP shall:

- (1) Identify by name, address and telephone number, the individual(s) who would notify the cognizant security office of such an occurrence, (the said individual(s) would not require access to classified information and therefore need not be cleared.); and
- (2) Include provisions for keeping the cognizant security office advised of the current combination to the container; and, in the case of one-person facilities of a multiple facility organization, keep the HOF security supervisor advised of the current combination to the container.

t. Special Access Programs. Shall implement Special Access Program requirements when such requirements are included in a DD Form 254 or other appropriate contract-related document.

u. Defensive Security Briefing.

- (1) Shall require all cleared employees (including cleared directors), Type A consultants, and temporary help supplier personnel, to inform him of their intended travel to or

through a Communist country,¹⁰ attendance at an international scientific, technical, engineering or other professional meeting, regardless of geographic location of such meeting, when it can be anticipated

¹⁰ Communist countries are: Albania, Bulgaria, Cambodia, Chinese Peoples Republic (Communist China) (including Tibet), Cuba, Czechoslovakia, Communist Korea (North Korea), German Democratic Republic (GDR) (East Germany, including the Soviet Sector of Berlin), Hungary, Laos, Mongolian Peoples Republic (Outer Mongolia), Poland, Rumania, Union of Soviet Socialist Republics (USSR) (including Estonia, Latvia, Lithuania, and all other constituent republics, Kurile Islands and South Sakhalin (Karafuto)), Vietnam and Yugoslavia.

that representatives of Communist countries will participate or be in attendance, or of plans to host an unclassified visit by representatives of Communist countries at a facility engaged in classified work or research. In instances where the individual is located at a using contractor or User Agency as a consultant or an employee of a temporary help supplier, the using contractor or User Agency, as appropriate, will be notified of the intended travel, attendance at a meeting, or hosting

of a visit. In the case of a facility where only one individual is located, the cognizant security office will be so informed. Where an individual works for more than one contractor or User Agency, each will be notified, and in the case of temporary help supplier personnel, the principal employer in addition to the using contractor or User Agency shall be notified.

- (2) Shall provide the individual or employee a defensive security briefing, based upon the guidance contained in Appendix VII. For temporary help supplier personnel, only one contractor or User Agency (where access is at the highest level) is required to accomplish the briefing. Usually the individual involved would be in the best position to determine which contractor or User Agency can most conveniently accomplish the briefing. Accordingly, the individual should make appropriate arrangements with that activity and furnish the other contractors or User Agencies at which he is employed, an advance notice stating when and by whom the briefing is to be given. Individuals and employees who frequently travel, attend meetings, or host visitors as described above, need not be briefed on each such occasion provided the individual or employee has been thoroughly briefed at least once within the preceding 6 months and reminded of his security responsibilities. Prior to departure of personnel for travel to or through a Communist country, or to attend a meeting outside the U.S., all classified information in their custody shall be accounted for by the using contractor or User Agency.
- (3) Shall, on completion of the briefing,

obtain from the individual or employee briefed a statement identifying who furnished the briefing and attesting that he understands his individual responsibility for safeguarding classified information. The statement of the individual or employee shall be retained for at least 3 years where the employee has had access to TOP SECRET, CRYPTOGRAPHIC or Special Access information, and for at least 2 years where access has been to SECRET or CONFIDENTIAL information. In the case of temporary help supplier personnel, the statement shall be forwarded to the temporary help supplier for retention. If the User Agency or cognizant security office conducts the briefing, they are responsible for obtaining the briefing statement.

- (4) Shall submit a report as required by paragraph 6b(9), unless the User Agency or cognizant security office conducted the briefing, in which case they shall submit the report.

v. Relationships With Citizens or Residents of Communist Countries.¹⁰

- (1) Shall require all cleared employees, including those in the process of being cleared by the DoD, to immediately notify the contractor who shall submit a report to DISCO in accordance with paragraph 6b(4), if either or both of the following events should occur subsequent to the completion of the employee's personnel security clearance forms:
 - (a) When a member of the immediate family of the employee or the employee's spouse takes up residence in a Communist country; or

(b) When, through marriage, the employee acquires relatives who are citizens or residents of a Communist country.

- (2) Shall require all temporary help supplier personnel, while such personnel are working under the contractor's direction and control on the using contractor's classified programs or contracts, to immediately notify the contractor if either or both of the events in paragraphs (a) and (b) above should occur. In such a case, the contractor shall then take action to ensure that the temporary help supplier is notified so that he can take action to submit a report to DISCO in accordance with paragraph 6b(4).

w. Emergency Procedure. Shall include in his SPP general instructions for safeguarding classified material in emergency situations such as a natural disaster or any civil disturbance. The procedure shall be as simple and practicable as possible and should be adaptable to any type of emergency that may arise. A procedure shall be incorporated in the SPP to provide for the submission of a report to the cognizant security office and contracting officer, by the most expeditious means, of any emergency situation which renders the facility incapable of safeguarding the classified material (see paragraph 6a(17)). Courses of action, not necessarily limited to the following, are available to the contractor to safeguard the classified material in his possession:

- (1) Secure the classified material in authorized storage containers or controlled areas. If feasible, a guard(s) should remain with material secured in controlled areas. The storage containers and controlled areas shall be examined upon return to the facility to determine whether the classified information has been compromised

or if any classified material is missing. A report shall be submitted in accordance with paragraph 6a(1) or (2) if appropriate.

- (2) Request assistance from appropriate civil authorities, including local and State law enforcement agencies.
- (3) Seek legal remedies such as the issuance of a court restraining order or injunction against interference with the contractor in the exercise of his property rights or in the discharge of his contractual obligation to safeguard classified information.
- (4) Request, when necessary, the assistance of the cognizant security office; for example: (i) in obtaining the legal remedies described in paragraph (3) above; and (ii) in arranging for the removal and safekeeping of the classified material by either the cognizant security office, contracting activity or a military activity located at or near the facility.

x. Release or Transmission Outside Contractor's Facility. Shall obtain the approval of the contracting officer prior to release or transmission of TOP SECRET information outside a contractor's facility in every instance. With respect to SECRET and CONFIDENTIAL information, the contractor shall obtain the contracting officer's approval for release or transmission outside the contractor's facility, except in the following instances:

- (1) When release is required by the specific terms of the contract.
- (2) When it is necessary in the performance of the contract.
- (3) In connection with pre-contract

negotiations with prospective sub-contractors, vendors or suppliers.

- (4) In prime contractor-subcontractor, multiple facility, and parent-subsidiary relationships as authorized by Sections VI and VIII, respectively.
- (5) During visits among prime contractors which are participating under Government direction in contracts pertaining to research, development or production of a weapons system (see paragraph 3bw).

When a contract requires classified material to be disseminated by a contractor to another contractor in accordance with a standard mailing or distribution list, and there is no current contractual relationship of a classified nature between the contractor and a designated recipient, the releasing contractor shall verify the facility security clearance and safeguarding capability of the recipient prior to making the first release of any material, except when advised by the contracting activity supplying the distribution list that it will retain the responsibility for these determinations. If appropriate, the cognizant security office of the recipient shall be advised by the releasing contractor that classified material will continue to be disseminated to the recipient under terms of the contract (identify the contracting activity and contract number) for a specified period (not to exceed the estimated date of contract completion or renegotiation), unless advised by the cognizant security office of a change adversely affecting the recipient's facility security clearance or safeguarding capability. When the mailing or distribution list requires dissemination of the material to a User Agency installation, the foregoing requirements do not apply, but the material shall be transmitted in accordance with paragraph 17.

y. DoD Technical Information Dissemination Activities. Shall forward the Facility

Clearance Register (DD Form 1541) which replaces DDC Form 20, to the cognizant security office when making the first or initial application for access to classified scientific and technical information in the possession of the DDC, Cameron Station, Alexandria, Virginia 22314, its field extensions, a DoD information analysis center or the Redstone Scientific Information Center, U.S. Army Missile Command, Redstone Arsenal, Alabama. This form is used to obtain certification of the category of classified material which an applicant (contractor) is cleared to receive and is capable of safeguarding. A DD Form 1541 shall be submitted only when requesting approval of the first Registration for Scientific and Technical Information Services (DD Form 1540) which replaces DDC Form 62. When certified, the DD Form 1541 remains in effect for all future registrations and until the contractor's facility security clearance is suspended, revoked or terminated, or until the contractor is no longer able to safeguard classified material at the specified category. The DD Form 1540 shall be submitted to the sponsoring User Agency contracting officer in accordance with guidance provided by DDC. Scientific and technical information acquired from DDC, its field extensions, a DoD information analysis center or the Redstone Scientific Information Center shall be safeguarded in accordance with the requirements of this Manual and the restrictions on the use, disclosure and dissemination of the information which are marked on the documents. When the contract to which the DD Form 1540 applies is completed or terminated, the contractor shall either destroy the material in the manner prescribed in paragraph 19 or obtain authorization to retain the documents from the sponsoring User Agency in accordance with paragraph 5m. The placing of an appropriate notation on each document, indicating the specific contract to which it pertains, will assist in achieving compliance with this requirement. DDC Forms 20 and 62, certified prior to 1 January 1966 need not be recertified.

z. List of Classified Contracts. Shall, after receiving notice of a forthcoming security inspection, prepare a listing of all classified contracts on which the facility is currently performing.

*aa. Investigative Assistance.*¹¹ Shall cooperate fully with representatives of Federal investigative agencies and of the cognizant security office conducting official investigations pertaining to the unauthorized disclosure of classified information or concerning the eligibility of personnel requiring access to User Agency classified information. This should include providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours and making employment and security records available for review upon request by such representatives and otherwise rendering assistance as necessary.

ab. Temporary Help Supplier Personnel. Shall orient temporary help supplier personnel in the security practices and procedures of the facility which will enable such personnel to understand and comply with the procedures applicable to the duties which they are to perform. The using contractor will also submit, as appropriate, reports pertaining to such personnel while they are actually working at his facility under his direction and control. This action by the using contrac-

¹¹ When reports are submitted or information is provided pursuant to these requirements, either classified if qualified, or offered in confidence, and so marked by the contractor, applicable exemptions to the Freedom of Information Act will be invoked as a matter of policy to withhold the information contained in such reports from public disclosure. When any of the reports submitted pursuant to these requirements contain unclassified information pertaining to an individual, the Privacy Act of 1974 permits the withholding of that information from that individual only to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. In appropriate cases the DoD will entertain a request from a defense contractor or its employees for such assistance as may be necessary against a legal action based on the reporting of information in accordance with the requirements of this Manual. Such assistance may include support for a claim by the contractor or the employees concerned that the information was reported under an absolute or qualifying privilege. In such cases the DoD will request appropriate assistance from the Department of Justice.

tor in no way relieves the temporary help supplier from complying with the requirement for security indoctrination and training of his employees or other concurrent requirements of this Manual.

ac. Self Inspections. Shall conduct his own self-inspection program for the purpose of evaluating all security procedures applicable to the facility's operations. The contractor shall review his security system on a continuing basis and shall also schedule a formal self-inspection so as to occur at a reasonable interval, i.e., midway between regularly scheduled Government inspections conducted by the cognizant security office. The inspection may be conducted by a security representative(s) from the facility or by a home office of cleared parent representative(s) at the discretion of management. In any event, management shall establish, at an appropriate organizational level, a procedure for evaluating the effectiveness of the self-inspection program. Self-inspections shall consist of an audit of all of the facility's operations in light of its SPP and the requirements of this Manual. As a minimum, self-inspections will include all elements normally inspected by the cognizant security office. Deficiencies identified as a result of self-inspections shall be corrected as expeditiously as possible. In the event difficulty is encountered in resolving a deficiency, the cognizant security office will provide assistance upon request. The contractor shall maintain a record of the dates upon which the self-inspection has been accomplished, and this record must be available for review during the next regularly scheduled inspection by the cognizant security office.

6. Reports

*a. The contractor shall submit immediately in writing to the cognizant security office—*¹²

¹² When the facility or contractor activity is located on a User Agency installation, and the Commander or Head of that installation is performing certain prescribed functions of a cognizant security office, the original copy of the report shall be furnished to the Commander or Head of the installation with an information copy of the report furnished to the cognizant security office.

→ (1) *Espionage, Sabotage, or Subversive Activities.* An information copy of any report filed under paragraph 6c with the FBI.

(2) *Loss, Compromise or Suspected Compromise.* A report, classified if appropriate, of any loss, compromise (including deliberate compromise) or suspected compromise of classified information.¹¹

(3) *Other Security Violations.* A report, in addition to the requirement of paragraph (2) above, classified if appropriate, of each violation of the requirements of this Manual involving TOP SECRET or Special Access information, RESTRICTED DATA, or COMSEC information, regardless of classification, which the contractor possesses in connection with User Agency contracts or programs.¹¹

(4) *Changed Conditions.* A report of:

(a) Any change of ownership, including stock transfers that affect control of a corporation.

(b) Change of operating name or address of the facility(s) covered by the DD Form 441.

(c) Any change in officers, directors, partners, regents, trustees or executive personnel, including, as appropriate, the names of the individuals they are replacing. In addition, a statement shall be made indicating (i) whether the new officers, directors, partners, regents, trustees, or executive personnel are cleared, and if so, to what level and when, their date and place of birth, and their citizenship; (ii) whether

they have been excluded from access in accordance with the provisions of paragraph 22e; or (iii) whether they have been temporarily excluded from access pending the granting of their personnel clearance.

(d) Any OODEP who becomes a representative of a foreign interest as defined in paragraph 3bb or whose status as a representative of a foreign interest changes in a manner that would make him ineligible for a personnel security clearance pursuant to paragraph 20k.

(e) Action to terminate business for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the DD Form 441.

(f) Any change which affects the information previously reported by the contractor on the Certificate Pertaining to Foreign Affiliation (DD Form 441s). This report will be made by the submission of a revised DD Form 441s. Moreover, when entering into discussions or consultations with foreign interests which may reasonably be expected to lead to the introduction or increase of FOCI and necessitate the submission of a revised DD Form 441s, the contractor shall report the details by letter. Additionally, when the contractor becomes aware of negotiations for the sale or transfer of securities to a foreign interest and such sale or transfer

would necessitate the submission of a revised DD Form 441s, the details will be reported by letter. Reports made pursuant to the foregoing are presumptively proprietary and will be protected from unauthorized disclosure and handled on a strict need-to-know basis. When such reports are submitted in confidence, and so marked, applicable exemptions to the Freedom of Information Act will be invoked to withhold them from public disclosure. (In cases where the contractor considers the information to be particularly sensitive or delicate and wishes to further restrict dissemination, the foregoing report may be appropriately marked and submitted to the Executive Director, Industrial Security, HQ DLA-N, Room 8A392, Cameron Station, Alexandria, Virginia 22314, in lieu of the cognizant security office.)

- (5) *Change in Closed or Restricted Areas.* A report of any change, in the location of Closed or Restricted Areas established under the provisions of Section IV, including the creation of any new areas requiring approval of the cognizant security office.
- (6) *Change in Storage Capability.* A report of any change in the storage capability which would raise or lower the level of classified information which the contractor is able to safeguard. (This provision does not require the contractor to

report the acquisition of additional containers approved for storage at the same level as that previously reported to the cognizant security office.)

- (7) *Employee Information in Compromise Cases.* A report, upon the written request of the cognizant security office, of information concerning any employee working in any of his plants, factories, or sites where work for a User Agency is being performed, when the information is needed in connection with the loss, compromise or suspected compromise of classified information.
- (8) *Category of Classified Information.* A report of the highest classification category of classified material received or generated at the facility. However, when the classification of the material received or generated is no higher than that of the material in possession of the facility during the last inspection or previously reported pursuant to this paragraph since the last inspection, an additional report need not be submitted.
- (9) *Termination Statement.* A report, in accordance with paragraph 5g, when an employee refuses to execute DLA Form 482.
- (10) *Delay in Shipment.* A report, in accordance with paragraphs 17c(5)(d) and 17d(3)(d) of the delay in the movement of classified material by commercial carriers of more than 48 hours after the expected time of arrival.

- (11) *Evidence of Tampering.* A report, in accordance with paragraph 12e (2) or 17g, of evidence of tampering with a shipment containing classified material.
- (12) *Improper Shipment.* A report when a classified shipment is received by other than an approved method prescribed by paragraph 17.
- (13) *Badges and Identification Cards.* A report, in accordance with paragraph 8c, which will inform the cognizant security office of the adoption of a new or revised employee badge or identification card system.
- (14) *Authorization to Apply Classifications.* Upon request, a report in accordance with paragraph 10e(4) of the number of individuals currently authorized by the contractor to apply a classification to information at each of the following categories: TOP SECRET, SECRET, and CONFIDENTIAL.
- (15) *Location or Disposition of Classified Material Terminated From Accountability.* A report, in accordance with paragraph 12h(2), when the whereabouts or disposition of classified material previously terminated from accountability is subsequently determined.
- (16) *Inability to Safeguard Classified Material.* A report, by the most expeditious means, of any emergency situation such as a natural disaster or civil disturbance which renders the facility incapable of safeguarding all classified material (see paragraph 5w). A report shall also be provided to all contracting officers concerned. This requirement of the DoD does not preclude similar reporting of the incident to appropriate local, State, and Federal civil authorities as the situation warrants.
- (17) *Annual Reports of OODEPs.* An annual report of OODEPs required to be cleared in connection with the facility security clearance pursuant to paragraph 22. The report shall designate by name those individuals granted a Letter of Consent (DISCO Form 560), those who are being processed for a security clearance, and those who have been excluded from the requirements for a security clearance pursuant to paragraph 22e. The report shall also contain, as appropriate, the information specified in paragraph 6a(4)(c) for each individual. The report shall be signed by an OODEP of the facility.
- (18) *Foreign-Classified Contracts.* A report of any precontract negotiation or award of a foreign or NATO contract from a foreign firm or government involving either U.S. or foreign classified information which is not placed through a User Agency.
- (19) *Receipt of Classified Material Not Related to a Classified Contract, Project or Program.* A report of the receipt of classified material which is not related to a contract, project or program and for which no specific safeguarding and disposition instructions have been received; further, if the contractor has been unable to obtain classification guidance or disposition instructions from the Government originator, or the Government activity releasing the material, the report shall so state. The report should identify the material by source, originator, quantity, subject or title, date and classification category.

b. The contractor shall submit the following reports immediately to the DISCO, Columbus, Ohio 43216, unless the individual involved is or was required to be cleared in connection with the facility security clearance pursuant to paragraph 22, in which case the report will be submitted to the cognizant security office.¹²

- (1) *Adverse Information.* A report, classified if appropriate, of any information coming to his attention concerning any of his employees who have been cleared or who are in the process of being cleared for access to classified information, which indicates that such access or determination may not be clearly consistent with the national interest. The subsequent discharge of an individual by the contractor who receives this information does not obviate the requirement to submit this report. In addition, if the individual is employed on a User Agency installation, a copy of such report shall be furnished to the Commander or Head of the User Agency installation. Where the employee concerned had been granted a CONFIDENTIAL clearance by the contractor in accordance with paragraph 24b, and is not in process for a Government granted security clearance, the clearance forms specified in paragraph 26c shall accompany the report of adverse information. This requirement to submit information reports also applies to cleared temporary help supplier personnel or Type A consultants utilized by the contractor. This requirement in no way affects the temporary help supplier's responsibility for submission of such reports when adverse information regarding his employee is brought to his attention.

- (2) *Change in Employee's Status.* A report of the death, the change in

name or the termination of employment of those employees who have been or are in the process of being cleared by the DoD for access to classified information, or who have taken residence or assignment outside the U.S., Puerto Rico, Guam or the Virgin Islands for a period in excess of 90 consecutive days during any 12-month period. Contractor employees visiting under Section V., are not included under provisions of this paragraph. Such changes will be reported by submission of a Personnel Security Clearance Change Notification (DLA Form 562-R). If the individual is reemployed within a 12-month period, DISCO shall also be notified immediately. Clearances may not be reinstated after the 12-month period has elapsed. Additionally, if it is subsequently determined that an employee who is in the process of being cleared by the DoD will not require access, DISCO shall be notified immediately so as to permit termination of the investigative action. When an individual is placed in a temporary lay-off status, a report of termination of employment is not required provided reemployment occurs within 12 months.

- (3) *Official Investigation.* A report upon the written request of DISCO, of information concerning any employee working in any of his plants, factories, or sites where work for a User Agency is being performed when the information is needed in connection with an official investigation.
- (4) *Relationships in Communist Countries.* A report in accordance with paragraph 5v, of the establishment of a relationship between a cleared employee, or one that is in the

process of being cleared by the DoD and a citizen or resident of a Communist country.

(5) *Representative of a Foreign Interest.* A report of any cleared employee (including those in the process of being cleared by the DoD), except those covered by paragraph 6a(4), who become representatives of a foreign interest as defined in paragraph 3bb or whose status as a representative of a foreign interest changes in a manner that would make him ineligible for a personnel security clearance pursuant to paragraph 20k.

(6) *Changed Intentions and Foreign Residence or Assignment of Immigrant Aliens.* A report of (i) residence or the assignment of a cleared immigrant alien outside the U.S. (including Puerto Rico, Guam or the Virgin Islands). Such individuals on visits of 90 consecutive days or less to foreign areas are not considered to be assigned outside the U.S., or (ii) a change in the intention of a cleared immigrant alien to reside permanently in the U.S., Puerto Rico, Guam or the Virgin Islands. An immigrant alien's change of intent to reside permanently in the U.S., and residence or the assignment of an immigrant alien outside the U.S., Puerto Rico, Guam or the Virgin Islands negates the basis (see paragraph 25) upon which the Letter of Consent was issued, and the Letter of Consent will be administratively terminated without prejudice by DISCO upon receipt of contractor notification. Except in connection with visits of 90 consecutive days or less in any 12-month period immigrant aliens may not be authorized access to classified information

when visiting outside the U.S., Puerto Rico, Guam or the Virgin Islands. Visits in excess of 90 consecutive days duration, in any 12-month period, shall invalidate any existing clearance.

(7) *Citizenship by Naturalization.* A report of a cleared immigrant alien who becomes a citizen through naturalization. This report will be made by the Personnel Security Clearance Change Notification (DLA Form 562-R), setting forth in the "Remarks" block (i) city, county and State where naturalized; (ii) date naturalized; (iii) court and, (iv) certificate number. Upon receipt of such a report, DISCO will issue a new Letter of Consent (DISCO Form 560).

(8) *Category 5 Visit Authorization.* A report of the termination of a Category 5 visit authorization, in accordance with paragraph 41e, when the requirement for such authorization ceases to exist prior to the expiration of the period for which it is valid.

(9) *Travel or Attendance at Meeting.* A report in accordance with paragraph 5u, upon completion of travel to or through a Communist country, or attendance at an international meeting outside the U.S. when Communist representatives participated or attended. The report shall include the employee's full name, clearance status, date and place of birth, a brief description of the projects, including the category of classified information, to which he had access during the past 2 years (depending upon the period of employment or utilization by the contractor in the case of temporary help supplier personnel),

CH 1

DoD 5220.22-M

the countries visited or the meeting attended, the dates of the travel and the employee's statement of the purpose and objective of the travel. The report shall include, if appropriate, a narrative statement of the circumstances surrounding all hostile intelligence efforts to obtain information from or to compromise the traveler, or of any endeavor by an unfriendly interest to establish a continuing relationship with the employee.

- (10) *Employees Desiring Not to Perform on Classified Work or Accept Security Responsibility or Requests to Terminate Clearance or Clearance Processing.* A report upon notification by an employee that he no longer wishes to be processed for a clearance pursuant to paragraph 26, or to continue an existing personnel security clearance.

→ c. The contractor shall submit immediately, in writing,¹³ to the nearest field office of the FBI a report, classified if appropriate, containing any information coming to his attention concerning existing or threatened espionage, sabotage, or subversive activities at any of his plants, factories, laboratories, or other sites, at which work for any User Agency is performed, or at which related material is acquired, stored, fabricated, or manufactured, or is in process of research or development.

7. Loss, Compromise, or Suspected Compromise of Classified Information

a. The contractor shall establish a procedure to insure that each loss, compromise, or suspected compromise of classified information and each failure to comply with a requirement of this Manual is immediately re-

ported to the facility security supervisor. Classified material which is out of the control of its custodian or which cannot be located shall be presumed to be lost until an investigation determines otherwise.

b. The contractor shall establish such procedures as are necessary to insure that any employee discovering the loss, compromise, or suspected compromise of classified information outside a facility promptly reports such a fact to:

- (1) The nearest office of the FBI and furnish sufficient information to assist in identification of the information. If the loss, compromise, or suspected compromise occurs outside the U.S., the nearest U.S. authorities shall be notified in lieu of the FBI; and
- (2) The facility security supervisor, by the fastest means of communication, who will then comply with paragraph c, below.

c. Immediately upon receipt of a report in accordance with paragraphs a, or b, above, the contractor shall initiate a preliminary inquiry to ascertain all of the circumstances surrounding the reported loss, compromise, suspected compromise or failure to comply with a requirement of this Manual. In the event of loss, a thorough search shall be conducted for the classified material.

d. If the contractor's inquiry prescribed in paragraph c, above, confirms (i) that a loss, compromise, or suspected compromise of any classified information occurred, or (ii) that a violation of a requirement of this Manual involving TOP SECRET, COMSEC Special Access information, or RESTRICTED DATA occurred, the contractor immediately shall submit a report of the incident to the cognizant security office in accordance with paragraph 6a(2) or 6a(3), as appropriate, and conduct a complete investigation of the

→ ¹³ If time is of the essence and the initial report is made via phone to the FBI, it must be followed in writing regardless of disposition made of the report by the FBI.

incident unless otherwise notified by the cognizant security office. Submission of the report shall not be deferred pending completion of the contractor's investigation.

e. Upon completion of the investigation prescribed in paragraph d, above, a final report shall be submitted to the cognizant security office referencing the preceding preliminary report, and containing the following:

- (1) A resume of the essential facts surrounding the incident, such as where, when and how it occurred, and what were the contributing factors.
- (2) The name and position of the individual(s) who was primarily responsible for the incident, including a record of prior loss, compromise, suspected compromise, or failure to comply with the requirements of this Manual for which the individual had been determined responsible.
- (3) A statement as to the corrective action taken to preclude a recurrence of similar incidents and the disciplinary action taken against the responsible individual(s), if any.
- (4) Specific reasons for reaching the conclusion that (i) loss or compromise occurred, (ii) compromise is suspected, (iii) the probability of compromise is considered remote, or (iv) compromise did not occur. In reporting the loss or compromise of classified material, sufficient descriptive data shall be furnished to permit the User Agency concerned to properly identify the material involved, such as originating activity or contractor, date of origin, document title, number of pages, description of contents, and the contract or program under which the material was received or produced.

8. Badges and Identification Cards

a. *Employee Badges.* Provided the contractor deems it necessary, he may use identification cards or badges to assist in identifying the level of security clearance of the holder and/or to indicate that the holder is authorized to enter Closed or Restricted Areas. If identification cards or badges are used for such purposes, the following shall apply:

- (1) The minimum identifying information to be shown on employee's identification badges or cards shall be the name and photograph of the holder. Other descriptive information to identify the authorized holder may be included on badges and/or cards at the option of the contractor.
- (2) The identification badge or card may include color or symbol coding to indicate the level of security clearance of the holder and/or that he is authorized to enter a Closed or Restricted Area, or a separate coded badge or card may be used for such purposes. When the combination of badges and/or cards are used, both must bear correlating data such as the same registration number or the name of the holder. However, where classified material is released to an employee (e.g., at a control station, blueprint crib, technical library) or entry into a controlled area is permitted on the basis of identification credentials, the verification of the credentials, (whether card, badge or combination thereof) shall include a check or the minimum identifying information prescribed in paragraph (1) above.
- (3) The words TOP SECRET, SECRET or CONFIDENTIAL, or abbreviations thereof, shall not appear on the badges or identification cards.

- (4) The makeup and construction of badges and identification cards shall be designed to minimize the possibility of tampering or unauthorized use.
- (5) Badges and identification cards, coded to indicate the level of security clearance or access to Closed or Restricted Areas, shall be rigidly controlled and accounted for by the contractor by use of a numbering system. Such controls shall apply equally to permanent and temporary cards and badges. Badges and identification cards shall be promptly recovered, or when appropriate, recoded whenever an employee's requirement for access or entry to a controlled area no longer exists due to an internal transfer, termination of employment, revocation of security clearance, or for other appropriate reasons.
- (6) Coded badges and cards shall be considered only as an aid in determining the current level of personnel security clearance of the holder or the areas to which the holder may have access. The clearance status of a person who holds such a badge or identification card shall be verified when there is doubt as to the validity of the badge or card.
- (7) An employee badge and/or identification card may be issued to persons referred to in paragraphs 37h and 41a.

b. Visitor Badges. A badge of such design as the contractor considers suitable may be issued to assist in identifying visitors who are authorized to be present in Closed or Restricted Areas. Visitors' badges, except for those issued in accordance with paragraph a(7), above, shall not be used to indicate the visitor's security clearance status. Visitors' badges shall be recovered at the

conclusion of the visit and they shall be rigidly controlled and accounted for by the contractor.

c. Reporting. The procedure for the use of badges or identification cards as authorized in paragraphs a and b, above, shall be incorporated in the SPP. In addition, the adoption of a new employee badge or identification card or any change in an existing badge or identification card shall be reported to the cognizant security office in accordance with paragraph 6a(13).

d. Use on User Agency Installations. The use of badges or identification cards to indicate the level of personnel security clearance of individuals performing duties within a User Agency installation shall be subject to regulations which apply to the installation.

9. DoD Sponsorship of Meetings

Meetings described in paragraph 5q(3) which serve a Government purpose and at which adequate security measures have been provided for in advance may be sponsored.

a. Requests for Sponsorship. A contractor desiring to conduct a meeting requiring DoD sponsorship shall submit his request to the DoD activity having principal interest in the subject matter of the meeting. Only one activity may sponsor a meeting on behalf of the DoD. Therefore, a request shall be sent only to one DoD activity at a time. If that activity declines to accept sponsorship, or if it should be appropriate to change the sponsoring agency, the request may be sent to another DoD activity having a principal interest in the subject matter of the meeting. Such requests shall include the details concerning all prior requests. Approval and sponsorship by the DoD will normally be granted only for a meeting conducted by a cleared DoD contractor. However, a meeting conducted by an association, society, or group whose membership consists primarily of cleared DoD contractors may be sponsored, provided a cleared contractor is designated and accepts overall security responsibility on behalf of the association,

society or group for the meeting. The request shall explain how the interests of national defense will be served by disclosing classified information at the meeting, and why the use of conventional channels for release of the information will not accom-

plish the purpose of those interests. The request shall also include a list of any foreign nationals or representatives of foreign interests (individual, firm, or government) whose attendance at the meeting is required.

b. *Attendance of Foreign Nationals or Representatives of a Foreign Interest.*¹⁴ No invitation, written or oral, shall be tendered to a foreign national, or to a representative of a foreign interest, to attend any session of a meeting sponsored by a DoD activity until approval for his attendance has been received from the sponsoring activity. If the attendance of a foreign national or representative of a foreign interest is required, a written request in advance of the meeting shall be submitted and shall include—

- (1) Identification of the foreign national or representative of a foreign interest by name, nationality, and government, individual or firm represented.
- (2) Sessions or subject matter for which access authorization is desired. (Nationals or representatives of Communist countries shall be excluded without exception, from attendance at any classified session.)
- (3) Subject titles of scientific, technical, and other papers scheduled for presentation by any foreign national or representative of a foreign interest.

c. *Location of Meetings.* The sponsoring activity is responsible for evaluating and approving the location proposed for the meeting.

- (1) Meeting at which TOP SECRET or SECRET information is to be disclosed shall be held only at a U.S. Government installation or at an appropriately cleared facility of a contractor which has adequate

means for safeguarding classified presentations. Under this criteria, the proposed site would have to be located within the physical boundaries of a cleared facility as indicated on the Facility Security Clearance Survey (DD Form 374). An auditorium, assembly hall, or gymnasium which is used primarily for campus activities and public gatherings will not be approved for a classified meeting at which TOP SECRET or SECRET information would be disclosed, even though it is located on the campus of a college or university, portions of which are a cleared facility.

- (2) Meetings at which information classified no higher than CONFIDENTIAL is to be disclosed shall normally be held on a U.S. Government installation or at a cleared facility. However, if suitable facilities are not available at a Government installation or contractor facility, the use of other locations may be approved provided adequate security can be maintained. Contractor requests to use a location other than a Government installation or contractor facility shall include—

- (a) A justification of the proposed location;
- (b) An explanation why a Government installation or cleared facility cannot be used; and
- (c) An explanation why separate classified and unclassified sessions cannot be scheduled, thereby permitting the use of a Government installation or a cleared facility for the classified portions of the meeting.

d. *Security Procedures.* When sponsorship of a meeting has been accepted by a DoD

¹⁴ Persons granted Canadian or U.K. Reciprocal clearances, and representatives of foreign interests cleared for access to classified information under the Department of Defense Security Program, are not subject to the limitation of paragraph 9b. However, persons granted Canadian or U.K. Reciprocal clearances are subject to the access limitations prescribed in paragraph 31.

activity, the contractor shall develop the security measures and procedures to be used and obtain the sponsoring activity's approval thereof. The security measures shall include adequate arrangements for—

- (1) Strictly limiting attendance at classified meetings to those persons whose presence is necessary in the interest of national defense, and who are otherwise eligible. This shall include measures for—

- (a) Determining and assuring that all persons selected and approved to attend classified sessions have been granted a security clearance for access to classified information equal to or higher than the category of information to be disclosed, and have duties in connection with a classified contract or program that requires such access in promoting the interests of national defense. For contractor personnel, the certification of security clearance and need-to-know shall be accomplished as provided in paragraph *f*, below.

- (b) Review and approval by the sponsoring activity of all announcements and invitations related to the meetings and lists of attendees pertaining thereto. Announcements and invitations shall be unclassified, and shall include the name of the sponsoring activity and the date of the approval.

1. Notices and announcements of meetings, whether classified, unclassified, or mixed, and not amounting to invitations to attend, may be published publicly, provided classified information is not

included in such notices or announcements.

2. In the case of classified meetings, invitations to attend (whether on an individual or class basis) shall not be sent to a person known to be from or a representative of a Communist country.

3. In the case of mixed meetings, i.e., those having both classified and unclassified sessions, the restrictions as to invitations to persons known to be from or representatives of a Communist country to attend are applicable to the classified session. As to the unclassified session, such notice or invitation to attend shall not be sent to persons known to be from or a representative of a Communist country unless and until specific authorization, on an individual name basis, has been made in advance by the Secretary or Head of the User Agency or his designee.

- (2) Safeguarding and controlling the distribution of notes, minutes, summaries, recordings, proceedings, and reports on the classified portions of the meeting. Such material shall normally be sent only to those approved for attendance at the classified sessions. However, the sponsoring activity may also authorize distribution to others who are determined to be eligible for, and require access to, the classified information involved. In any event, the material shall only be sent to a Government activity or cleared contractor facility and marked for the

attention of the intended recipient, as provided for in paragraph 17k.

- (3) Notifying each person who presents or discloses classified information at the meeting of the security limitations on disclosures for such reasons as the level of clearance or need-to-know of members of the audience or other limitation established by the Government.
- (4) Assuring the physical security of the meeting site and the area used for classified sessions or displays. This shall include provisions for guards, entrance controls, personnel identification, storage facilities, and adequate security against unauthorized access to, or illicit acquisition of, the classified information.
- (5) Insuring that attendance at a meeting or session at which classified information is to be disclosed is limited to persons whose names appear on an approved access list, and then only upon proper identification.
- (6) Submitting the minutes, summaries, recordings, proceedings, and reports of the meeting to the sponsoring activity for security review and for approval of the distribution proposed therefor.
- (7) Assuring that individuals making oral presentations at meetings provide classification guidance sufficient to enable attendees to identify what information is classified or unclassified, and if classified, at what category or categories of classification.

e. Requests for Disclosure Authority. A contractor desiring to disclose classified information at a meeting as provided in paragraph 5q(3) or 5q(4) shall—

- (1) Obtain prior written authorization for each proposed disclosure of classified information from the contracting officer having jurisdiction over the information involved. If authorization for foreign nationals to attend the meeting has been requested from the sponsor, that fact shall be stated in the request for disclosure authority.
- (2) Furnish a copy of the disclosure authorization to the Government activity conducting or sponsoring the meeting.
- (3) Furnish a written copy of the presentation, as made, to the contracting officer and to the conducting or sponsoring activity if they are not one and the same.

f. Requests to Attend Classified Meetings. A contractor desiring to have an employee attend a classified meeting shall—

- (1) Certify to the clearance status of the employee who will attend the classified meeting.
- (2) Forward the application or request to attend the meeting, together with the necessary justification (see paragraph d(1)(a), above) to the contracting officer for the classified contract under which access is being justified, requesting that it be forwarded to the sponsoring activity following determination of the employee's need-to-know. However, where access is being justified under a User Agency program, rather than a contract, the request shall be forwarded for determination of need-to-know to the official of the User Agency activity who is monitoring the contractor's participation in the program.

SECTION II

HANDLING OF CLASSIFIED INFORMATION

10. Classification

a. The security classification to be applied to information involved in User Agency contracts and programs will be supplied by the contracting officer or his designated representative of the User Agency concerned. The DD Form 254, attachments and supplements, as appropriate, provide classification specifications to be used for this purpose. The completed DD Form 254 is the basic document for conveying to the contractor the classification, regrading, and declassification specifications for a classified contract. It is designed to identify by a combination of a check list and narration the specific items of classified information involved in the contract which require security classification protection. Contractors are encouraged to advise and assist in the development of the classification specification in order that their technical knowledge may be utilized and they may be in a better position to anticipate the security requirements under the contract and organize their procedural and physical plant layout accordingly.

b. An original DD Form 254, which sets forth the classification specification or cites the classification guidance in item 15, is provided to the contractor by the User Agency with an RFP, RFQ, IFB, or other solicitation and with the award of contract which will necessitate access to classified information. A revised DD Form 254 will be issued at any time a change or additional classification guidance is found necessary. The User Agency reviews the existing classification specification periodically during the contract and at least once annually. When the annual review establishes that no change is necessary in the existing specification, the prime contractor is advised in writing. A final DD

Form 254 is issued upon final delivery of goods or services or upon termination of the contract when authority is granted under paragraph 5m for the contractor to retain classified material originated by the User Agency or generated by the contractor in the performance of the contract, or when all classified material, for which retention authority would be required, is ordered immediately declassified. A final DD Form 254 is not issued, however, when authority is granted under paragraph 5m for the contractor to retain only reference material (see paragraph 3az.). Reference material is marked by its originator to reflect the automatic downgrading and declassification instructions. When it is not so marked, the contractor is responsible for applying the appropriate marking in accordance with paragraph A4, Appendix II.

c. When a final DD Form 254 is in effect, and at the conclusion of a retention period authorized under paragraph 5m, the contractor requests an extension of the retention period, the User Agency will conduct a review to insure that the contractor has a continued requirement for possessing the classified material and to revise the existing classification specification as necessary to cover classified material for which extension of retention authority is authorized.

d. The application of a security classification to information developed by the contractor shall be based on (i) the classification guidance furnished by the contracting officer of the User Agency in accordance with paragraph a., above, or (ii) the contractor's knowledge that such information is in substance the same as, or would reveal, other information known to be currently classified. Material developed by the contractor

CH 1

DoD 5220.22-M

containing classified information, or from which classified information could be obtained, shall be marked in the manner prescribed in paragraph 11.

e. The contractor shall establish a procedure to insure that:

- (1) In the case of a document, and except as specified in paragraph (3) below, the manager or supervisor, whose signature or other form of approval is required before the document may be issued, transmitted, or referred outside of the facility, determines the necessity, currency, and accuracy of the classification applied to that document.
- (2) In the case of material other than a document, and except as specified in paragraph (3) below, the manager or supervisor in charge at the operational level where the material is being produced or assembled determines the necessity, currency, and accuracy of the classification applied to that material.
- (3) In those situations involving the copying or extracting of classified information from another document, or involving the reproduction or translation of a whole classified document, the individual responsible for such copying, extracting, reproduction or translation marks the new document or copy with the same classification as that applied to the information or document from which the new document or copy was prepared.
- (4) Employees responsible for the currency, necessity, and accuracy of the classification applied to information under paragraphs (1) and (2) above are held to a minimum number consistent with operational re-

quirements. The number of such employees shall be reported to the cognizant security office upon request in accordance with paragraph 6a(14).

- (5) Questions on the currency of the classification of reference material are referred as indicated in paragraph 60i.

f. Whenever a contractor develops an unsolicited proposal or originates information not in the performance of a User Agency contract or program, the following rules shall apply:

- (1) If information is included in the proposal or other material which the contractor identifies as already being classified, the proposal or other material shall be marked with the appropriate classification in accordance with paragraph 11.
- (2) If the case does not fall within paragraph (1) above, and the contractor believes that the proposal or other material contains information which may or should be safeguarded, the contractor is requested to protect the information as though classified at the appropriate level, until an advisory classification opinion is obtained from a User Agency which has an interest in the subject matter. In any such case, the following protective marking, or a similar marking which clearly conveys the same meaning, will be used:

Classification determination pending.

Protect as though classified

(CONFIDENTIAL, SECRET or TOP SECRET)

This marking shall appear conspicuously at least once on the material, but it is not necessary to mark the material further in accordance with paragraph 11 until the advisory classification opinion is received. In addition, if applicable, contractors are not precluded from designating such information as company private or proprietary information.

(a) Pending determination by the User Agency, the following precautionary measures should be taken in regard to safeguarding such information:

1. Access to the information should be limited to the minimum number of personnel practicable.
2. Persons selected to have access to the information should be limited to U.S. citizens or immigrant aliens who are known to be trustworthy. They should be advised of the importance of the information.
3. When not in use, documents containing the information should be stored in a secure container.
4. In forwarding the information between persons or locations, a secure method of transmission should be used.
5. Reproduction of the information should be kept to a minimum.

(b) It is the general policy of the DoD not to classify information over which it has no juris-

diction. The proposal or other material shall not be classified by the User Agency (i) unless it incorporates classified information to which the contractor was given prior access, or (ii) unless the Government first acquires a proprietary interest (official information, see paragraph 3av).

g. The contractor shall provide security classification specifications to employees performing in a sales or technical capacity or under a classified contract outside of the U.S.

h. The fact that information currently classified by a User Agency has been disseminated by a public medium of communication does not automatically mean that it has been declassified. Classification shall be continued until advised to the contrary by the User Agency. Questions as to the propriety of continued classification in these cases should be brought to the immediate attention of the contracting officer.

11. Marking

The paragraph marking requirements in paragraph a., below are mandatory only with respect to documents transmitted outside a facility. If, in an exceptional situation, such marking is determined to be impracticable, documents shall contain a description sufficient to identify the exact information which is classified and the appropriate classification category(s) assigned to it.

a. *Initial Marking.* Classified material shall be marked with the date of origin, the name and address of the facility responsible for its preparation, and shall be plainly and conspicuously marked or stamped (not typed) with the appropriate classification. Each paragraph or subparagraph of the document shall be marked to show the cate-

gory of classified information it contains, or that it contains no classified information. However, individual paragraph/subparagraph markings are not required when all paragraphs/subparagraphs contained on a page of a classified document are unclassified and the page is so marked. The lead-in or basic portion of a paragraph which contains subparagraphs shall be marked to reflect the overall classification of the entire paragraph. The actual classification of the lead-in paragraph, when it is unclassified, or classified at a lower level than the overall paragraph, shall be shown at the end of the lead-in paragraph text. When different items of information in one paragraph require different classifications, but segregation of the information into separate paragraphs would destroy continuity of context, the highest classification required for that item shall be applied to the paragraph. In marking paragraphs, the appropriate marking shall be placed immediately preceding and to the left of the parts involved. The symbols (TS), (S), (C) and (U) for TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED will be used. When appropriate, the symbol (RD) for RESTRICTED DATA and (FRD) for FORMERLY RESTRICTED DATA shall be added. EXAMPLE:

(S) (FRD) This is an illustration of how a lead-in paragraph shall be marked when the overall paragraph classification of SECRET FORMERLY RESTRICTED DATA is different from the lead-in paragraph classification of CONFIDENTIAL. (C)

- (1) *Documents.* The overall classification of a document, whether it be a letter, report, message, pamphlet, etc., shall be conspicuously marked or stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, on the back page, and on the outside of the back cover (if any). Each interior page of a document, except blank

pages, shall be conspicuously marked or stamped at the top and bottom with the highest classification of the information appearing thereon, including the designation UNCLASSIFIED, when appropriate. Single sheet documents shall have the overall classification of the document affixed to both sides of the sheet. In some complex documents their major components are likely to be used separately. In such instances, each major component shall be marked as a separate document, utilizing the classification marking techniques described above. Examples include (i), annexes, appendices, or similar component, (ii) attachments or enclosures to a memorandum or letter, and (iii) each major part or chapter of a report. In the event a major component, as described above, is incorporated into a document prepared earlier and such document was previously unclassified or classified at a lower level than the component now being incorporated into the document, the overall classification of the document must be adjusted to reflect the higher level of classification for the information now within the document. Classification markings shall be so applied as to be clearly visible when pages are clipped or stapled together.

- (2) *Special Situations.* As an exception to the general rule, where printing is performed by the GPO or under contract to the GPO, or by a contractor in accordance with Government contract specifications, classified documents comprised of many pages (studies, manuscripts, reports, manuals, etc.) may have the overall classification shown on each page provided the classified and unclassified parts of that page are clearly identified to the recipient by paragraph markings or by other means set forth in the document. In such cases paragraph

marking or other means shall take precedence over page markings.

- (8) *Letters of Transmittal.* A letter transmitting classified information shall be marked with a classification as high as its highest classified enclosure. Letters of transmittal, when appropriate, shall bear a notation indicating that upon removal of the classified enclosures such letters may be downgraded or declassified. When a multiple page letter of transmittal contains no classified information, only the first page thereof need be marked with the classification of the highest classified enclosure.

- (4) *Artwork.* Original artwork shall have the security classification stamped or marked conspicuously in top and bottom margins of the mounting board and on all overlays and cover sheets.

- (5) *Charts, Maps, Drawings, and Tracings.* The classification shall be affixed under the legend, title block, or scale, and at the top and bottom, in such manner that it will be reproduced on all copies, except that in the case of drawings smaller than 17"x22" the classification need not be affixed under the legend, title block or scale, unless the classification assigned to the legend, title block or scale is different from that assigned to the overall drawing. If the information contained in the legend or title block is of a different category than that contained in the balance of the document, the abbreviations prescribed for subjects and titles in paragraph (9) below shall be placed under or alongside the classification marking affixed under the legend, title block or scale and the higher classification marking shall be placed at the top and bottom of the document. For example:

SECRET

(Legend Unclassified)

SECRET

(Drawing CONFIDENTIAL)

- (6) *Films, Microfilms, Microfiche, and Photographs.* Classified films and microfiche shall be marked in a fashion that will permit classification markings to appear in the projected image. In addition, holders or containers for all such material shall be conspicuously marked with the appropriate classification. Continuous cover aerial reconnaissance mapping negatives, microfilm in roll form, and motion picture films shall be marked with appropriate classification at the beginning and end of each roll. In addition, motion picture film shall state in the title frame the classification thereof. These and other classified negatives which do not lend themselves to marking shall be handled on a classified basis and shall be kept in containers, properly secured, which shall bear the classification marking to which the contents are entitled, the date of origin, and other notations required by paragraph b, below as appropriate. When using self-processing film or paper to photograph or reproduce classified material, caution must be exercised to assure the negative of the last exposure does not remain in the camera. The negative of the last exposure of such self-processing film or paper shall be removed and destroyed as classified waste, or the camera shall be protected as classified material. Photographs (positives and negatives) shall be marked with the appropriate classification, top and bottom, and where practicable, the center of the reverse side. Photo-

graph containers shall also be conspicuously marked with the appropriate classification.

- (7) *Sound, Magnetic and Other Recordings.* Classified sound, magnetic and other recordings shall be marked with the appropriate classification if practical. The containers in which such recordings are placed during non-use shall be marked conspicuously. For tapes and similar items, the marking normally shall be placed at the beginning and the end of the roll. However, such recordings which do not lend themselves to marking shall be handled on a classified basis and shall be kept in containers which shall bear the classification markings to which the contents are entitled. In addition, where practical, the applicable classification shall be incorporated into the recording at the beginning and end thereof in a manner which will assure that any person having access to the classified information contained therein, when reproduced by any medium, will know the classification of the information. In the case of disc or drum memory units utilized in electronic data processing equipment, which do not lend themselves to marking, the entire processing unit shall, when the memory units contain classified information, be marked in the manner prescribed by paragraph (8) below.

- (8) *Material.* Items of classified material shall be properly marked to indicate the classification of the information contained in or revealed by the material and which may be acquired through observation, study, analysis, use, or testing. However, classified material which does not lend itself to marking shall have securely affixed or attached a tag, sticker, decal, or similar device bearing the

classification, and the appropriate markings required by paragraph b., below. Where the foregoing is not practicable, the marking may be placed on or affixed to the container of the classified material in lieu of the material itself. During production and until marked as above, the contractor shall post notice in the area of production of the classification of the material to alert all personnel who will have access of the proper classification.

- (9) *Subjects and Titles.* On each classified document, the subject or title shall be followed by its own classification (or by the designation UNCLASSIFIED) in parentheses. For this purpose, the parenthetical abbreviations (TS), (S), (C), and (U) may be used, respectively, for TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED. (So far as possible, a classified document shall be assigned an unclassified subject or title.) When appropriate, the abbreviations for RESTRICTED DATA (RD) or FORMERLY RESTRICTED DATA (FRD) shall be added.

- (10) *Machine Listing.* Classification markings on pages of listing produced by automatic data processing equipment may be applied by the equipment, provided the first page, the back page, and the front and back covers (if any), are appropriately marked as otherwise prescribed. If individual pages are removed from a listing marked in this manner, each page so removed shall be marked as otherwise prescribed,

- (11) *Machine Accounting Cards.* A deck of classified accounting machine cards may be marked as a single classified document. A deck so

marked shall be stored, transmitted, destroyed and otherwise handled in the manner prescribed for other classified documents of the same classification. The first and last cards in the deck shall be marked to show the overall classification of the deck. In addition, the first card must identify the contents of the deck and the downgrading and declassification markings which apply to the deck. If it is not practical to mark the first card in the deck with the overall classification, identity of the contents of the deck and the downgrading and declassification marking applicable, an additional card, inserted at the beginning of the deck, may be used for such purpose. The individual cards of the deck need not be marked individually. Cards removed for separate processing or use, however, shall be protected to prevent compromise of any classified information contained thereon and, unless promptly returned to the deck after processing or use, shall be marked with the appropriate classification. When marked individually, the security classification shall be stamped, preprinted or machine printed above the 0 punch location and below the 8 punch location between card columns 54 and 76. Other markings prescribed by paragraph b, below, shall be placed on the back of the card.

- (12) *Messages.* The document which is prepared by the originator of a message and submitted to the communications center or activity for electrical transmission shall be marked in the manner prescribed by paragraph (1) above. In addition, the first word in the text of the proposed message shall be the classification of the message. When appropriate, the notations required by paragraphs b(2), (3) and (4) below shall immediately follow the classification

designation at the beginning of the text except that RESTRICTED DATA or FORMERLY RESTRICTED DATA shall be used for the notation prescribed in paragraph b(2) or (3) below, respectively. The last line or paragraph of the proposed message shall show the appropriate downgrading and declassification marking (see paragraph E, Appendix II). When transmitting the message by electrical means, the classification marking shall be included at the beginning of the encrypted text. The last line or paragraph of the transmitted message shall show the appropriate downgrading and declassification marking. Classified messages shall be marked at the top and bottom with the overall classification and shall be paragraph marked in the manner prescribed above for documents. A message printed by an automated system may have the classification markings applied by the system provided such markings are clearly distinguishable from the printed text. In addition, markings required by paragraph b., below shall be applied as appropriate.

- (13) *Classified Files.* File folders, binders, envelopes, etc., containing classified documents shall be marked or stamped with a classification equal to that of their highest classified contents. Documents removed from the file or group shall be handled in accordance with their individual classification requirements.
- (14) *Classified Compilations.* Where the use of a classification higher than that which applies to any of its components is required by the specific provision of the DD Form 254, or other User Agency direction, to protect a compilation of information, the overall classification shall be placed on the document in the manner pre-

scribed by this paragraph. Where the individual parts of a compilation are unclassified but their total content or their association is classified, the document shall be marked with the proper classification. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the document.

- (15) *Classified Translations.* Translations of U.S. classified information into a language other than English shall show the U.S. as the country of origin, and shall be marked with both the U.S. classification and the foreign language equivalent of the U.S. classification (see paragraph *d*, below). Conversely, translation of foreign classified information into English shall be marked with the name of the country of origin and the foreign and U.S. equivalent classifications. If the information was not classified by the country of origin, a U.S. classification shall be applied to the information only if it is required to protect the fact that the U.S. has possession of the information.

- (16) *Working Papers.* Working papers such as notes, drafts, drawings, etc., accumulated to assist in the formulation and preparation of a finished document, shall be marked with both the initial and the additional markings prescribed here in the same manner as other documents except the additional markings required by paragraphs *b*(1) and (5), below need not be affixed to working papers until the material is entered into the control station accountability records in accordance with paragraph 12, is made a part of a permanent record, or is dispatched outside of the facility. In the case of the RESTRICTED DATA and FORMERLY RESTRICTED DATA notations cited below,

there is no requirement for completing the CLASSIFIED BY line appearing on those markings until such subsequent time that the notation concerning downgrading or declassification must be affixed in accordance with the circumstances prescribed herein.

- (17) *Rolled or Folded Documents.* Classified documents are sometimes rolled, folded, or covered over in such a manner that the classification markings are obscured. When this occurs, the classification shall be marked, stamped or otherwise affixed to the exposed surfaces of the document so that it may easily be seen.

b. Additional Markings. In addition to the required classification markings, all classified material shall be marked, as appropriate, with one or more of the notations prescribed below. The appropriate notation shall be printed, stamped, typed, or otherwise affixed conspicuously at least once on all classified material possessed,¹ prepared or reproduced by the contractor. In addition, when a copy, extract, or paraphrase of a document contains national security information, or when a page, chapter or other such component is separated from a document, the extract or component shall also be marked conspicuously at least once with the appropriate notation.

- (1) *Unauthorized Disclosure Notation.* All classified material other than RESTRICTED DATA or FORMERLY RESTRICTED DATA, which is furnished to persons outside the Executive Branch of Government shall be marked with the notation shown below. If the classified item does not lend itself to marking, the recipient

¹ Whether or not removed from file or storage for any use, classified material pre-dating January 22, 1973 (date of promulgation of this footnote) which is already marked with officially prescribed additional warning notices which convey in substance the same meanings as those prescribed in paragraphs 11b(1) thru (4) need not be re-marked.

shall be notified in writing of the notation.

**NATIONAL SECURITY
INFORMATION**

Unauthorized Disclosure Subject to
Criminal Sanctions

- (2) *RESTRICTED DATA Notation.* The following notation shall be affixed on all material which contains Atomic Energy RESTRICTED DATA as defined in paragraph 3bd. If a document contains both RESTRICTED DATA and other classified information, the following notation shall be placed on the document instead of that shown in paragraph (1) above.

RESTRICTED DATA

This material contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Its dissemination or disclosure to any unauthorized person is prohibited:

Classified by:

- (3) *FORMERLY RESTRICTED DATA Notation.* All material containing information in the FORMERLY RESTRICTED DATA category as defined in paragraph 3af, but not containing Atomic Energy RESTRICTED DATA, shall be marked with the following notation instead of that in paragraph (1):

FORMERLY RESTRICTED DATA

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as RESTRICTED DATA in foreign dissemination. Section 144b, Atomic Energy Act 1954.

Classified by:

- (4) *Sensitive Intelligence Information.* Classified material which contains sensitive intelligence information will be marked with the following warning notice. This warning notice will be used in addition to, and in conjunction with, the marking prescribed in paragraphs (1), (2), and (3) above, as appropriate.

**WARNING NOTICE
SENSITIVE INTELLIGENCE
SOURCES AND METHODS INVOLVED**

- (5) *Notation Concerning Downgrading or Declassification.* Procedures governing marking for downgrading and declassification, or exemptions therefrom, are prescribed in Appendix II.

c. Marking of Regraded Documents and Material. Whenever classified material is downgraded, declassified or upgraded, the material shall be promptly and conspicuously marked to indicate the change, the authority for the action, the date of the action, the identify of the person or activity taking the action, and his operating entity, according to the following.

- (1) *Upgraded Material.* In every case, when material is upgraded, all the old classification markings shall be immediately cancelled and the new markings entered in accordance with the notice to upgrade the material. In the case of documents, the old classification markings shall be immediately cancelled on the outside of the front cover (if any), the title page (if any), the first page, the back page, and on the outside of the back cover (if any), and the new markings applied. Inside pages and paragraphs of documents shall be marked as specified in paragraph a(1) in accordance with the notice to upgrade.

(2) *Downgraded or Declassified Material.*

- (a) When the material is downgraded or declassified in accordance with the ADS or the GDS, specified in Appendix II, the notations prescribed by Appendix II constitute the authority for the downgrading or declassification action. All the old classification markings shall be cancelled and the new markings substituted, whenever practicable.¹ In the case of documents, as a minimum, the outside of the front cover, if any, the title page, the first page, the back page, and the outside of the back cover, if any, must reflect the new marking.² Prints of motion picture film shall show regrading action on leaders attached between the plain leader and the first title frame. Material such as negatives, standing type, proofs, etc., will have a statement

¹ In the interest of providing quick and efficient service on requests for classified documents, the following marking procedures are currently being used by the DDC:

(i) Except as indicated in paragraph (ii) below, documents which have been downgraded or declassified will only reflect such action on the front and back covers and the title, first and back pages. A notice will be affixed to the front cover or title page of such documents by DDC indicating that it is the responsibility of the recipient (the contractor who requested the document) to complete the marking of the regraded document in accordance with paragraph 11c(2).

(ii) Documents which were originally marked under the provisions of E.O. 10501 and which contain pages which do not bear any classification markings, will be marked by DDC prior to dispatch, with the overall classification of the document marked on each page. As a result, individual pages of the document may be assigned a higher classification than warranted by their contents. For this reason, contractors should direct any questions they may have concerning the classification of an individual page, chapter, section, etc., to the originator of the document before extracting or reproducing the information. A notation, reading substantially as follows and appearing on the front cover or title page, will alert contractors to the above situation: "This is a reproduction of a document, originally marked under the provisions of E.O. 10501, which, under certain circumstances, eliminated the requirement that interior pages be marked with their own individual classification. The DDC has marked each such page with the current overall classification of the document, in addition to the outside front cover and the outside of the back cover. The document and all of its pages or parts will be protected in accordance with this classification until the actual classification can be determined. Any question by the recipient as to the correct security classification of any particular portion of the document should be directed to the originator of the document."

showing the regrading attached thereto in a manner which will not alter the re-use of the material. The containers or holders for negatives, film, microfiche, etc., shall reflect the new markings, and any hard copy produced from such materials shall also reflect the new markings.

- (b) When the volume of material is such that prompt re-marking of each classified item cannot be accomplished without unduly interfering with operations, the custodian may attach downgrading and declassification notices to the inside of the file drawer or other storage container in lieu of the re-marking otherwise required. Each such notice shall specify the authority for the downgrading or declassification action, the date of the action, and the storage container to which it applies. All re-marking actions shall be in accordance with paragraph (a), above. When documents or other material subject to downgrading or declassification are withdrawn from one storage container solely for transfer to another, or when a storage container holding such documents or material is transferred from one place to another the transfer may be made without re-marking if the notice is attached to the new container or remains attached to the old container.

d. Marking of Foreign Classified Material.

Foreign classified material shall be marked in accordance with instructions received from the foreign contracting authority, the cognizant security office, or the User Agency. In any case, if the classification and the country of origin are in a language other than English, the appropriate equivalent U.S. classification and the country of origin

will be marked on the foreign classified material. These markings shall be applied to all classified material developed, produced, or reproduced by the contractor which is derived from the original foreign classified information. Markings shall be applied as prescribed in paragraph *a.*, above. Additional markings prescribed in paragraph *b.*, above shall not be used. Many foreign governments and international organizations, such as NATO, use a fourth security designation identified as "RESTRICTED" to denote a foreign requirement for security protection of a lesser degree than CONFIDENTIAL. Foreign RESTRICTED material shall be marked "RESTRICTED" together with the country of origin and protected in all respects in the same manner as U.S. CONFIDENTIAL, except that foreign RESTRICTED material may be stored in locked filing cabinets, desks, or other similar closed spaces which will prevent access by unauthorized persons.

12. Record of Classified Material

a. Accountability Records. The contractor shall maintain, at one or more control stations, an accountability record of all TOP SECRET and SECRET material, and CRYPTO regardless of classification. The record shall include all such classified material received or produced by, or in the possession or custody of, the contractor and shall reflect as a minimum (i) the date of receipt or origin, (ii) the activity from which received or by which originated (iii) the classification of the material, (iv) a brief, unclassified description of the material and (v) the disposition of the material and the date thereof (i.e., destroyed, downgraded to CONFIDENTIAL, declassified, dispatched outside the facility). These records shall be retained by the contractor for a minimum of 3 years for TOP SECRET material, Special Access material, and CRYPTO regardless of classification; and for SECRET material for 2 years from the date the last item recorded thereon was destroyed, downgraded to CON-

FIDENTIAL, declassified, dispatched outside the facility or transferred to another accountability record.

b. Inventory/Accounting of Classified Material. When directed by the Commander of the DCASR, the contractor shall make an inventory and accounting of all TOP SECRET and SECRET material, and CRYPTO regardless of a classification, and shall submit a report of all unresolved discrepancies to the cognizant security office. The inventory and accounting shall consist of the actual sighting of each item listed in the accountability records or an examination of the evidence of its proper disposition (the receipt, certificate of destruction, authorization to terminate from accountability, or record of downgrading or declassification); and an examination of the contents of all containers authorized for storage of classified material to assure that all TOP SECRET and SECRET material, and CRYPTO, regardless of classification, has been entered into the accountability records.

c. Receipt and Dispatch Records. In addition to the accountability records required in paragraph *a.*, above, the contractor shall maintain a record at one or more control stations of all non-accountable classified material received by or dispatched from the facility. This record shall reflect as a minimum: (i) the date of receipt or dispatch; (ii) the activity from which received or to which dispatched; (iii) the classification of the material; and (iv) a brief, unclassified description of the material. These records shall be retained by the contractor for a minimum of 2 years from the date of the last entry. However, if the contractor combines this record of receipt and dispatch with the accountability records prescribed in paragraph *a.*, above, for TOP SECRET material, Special Access material, and CRYPTO, regardless of classification, the 3-year retention period shall apply.

d. Control Station Personnel. Employees designated by the contractor to operate a control station shall be cleared at the same level as the facility at which they are as-

signed, except that such personnel will be required to have a TOP SECRET clearance only if the person's duties afford him access to or possession or custody of TOP SECRET material.

e. Receipt of Classified Material. When classified material is received at the facility, either by mail, bulk shipment or messenger, the following controls shall apply:

- (1) All classified material shall be delivered unopened to personnel designated by the contractor to receive it at the control station(s). In addition, when U.S. Registered Mail, U.S. Express Mail or U.S. Certified Mail or classified material delivered by messenger is not received directly by the designated control station personnel, procedures shall be established to assure that such mail is received by appropriately cleared and authorized personnel, for delivery with the inner container unopened to the control stations(s). In effect, all contractor personnel who handle U.S. Registered Mail, U.S. Express Mail, or U.S. Certified Mail shall be appropriately cleared.
- (2) The package shall be examined for any evidence of tampering and the classified contents shall be checked against the receipt. Evidence of tampering shall be reported immediately to the cognizant security office in accordance with paragraph 6a(11). Discrepancies in the contents of a package or absence of a receipt for TOP SECRET or SECRET material, and CRYPTO, regardless of classification, shall be reported immediately to the sender. If the shipment is in order, the receipt shall be signed and returned to the sender. For purposes of positive identification, the name of the employee signing the receipt shall be printed, stamped, or typed on the receipt. In those special cases where the sender elects to include a receipt form with CONFIDENTIAL mate-

rial, the receiver shall execute the receipt and return it to the sender if the contents of the package are in order.

f. Production of Classified Material. When a contractor produces TOP SECRET or SECRET material and CRYPTO, regardless of classification, accountability shall be established, as follows:

- (1) *TOP SECRET Documents and CRYPTO Documents, Regardless of Classification.* Such documents shall be entered into the control station accountability records when the first of any of the following events occurs: the document is retained after the next successive stage in its development is completed (e.g., notes converted to draft, final draft placed on masters, photographic prints developed from negatives, etc.); the document, including classified working papers, drafts, etc., is retained for more than 30 days from the date of origination; the document is reproduced for internal purposes (e.g., draft review, coordination) prior to preparation of final copy; or the document, regardless of stage of development, is transmitted outside of the facility on a temporary or permanent basis.
- (2) *SECRET Documents.* Such documents shall be entered into the control station accountability records when the first of any of the following events occurs: the document is retained as a completed document (including working papers) in excess of 30 days from the date of completion; the document is reproduced for internal purposes; the document is retained as a partially completed document on discontinuance of the work; or the document, regardless of stage of development, is transmitted outside of the facility on a temporary or permanent basis.
- (3) *Other Material.* TOP SECRET and SECRET material, and CRYPTO, re-

ardless of classification, in other than documentary form, shall be entered into the control station accountability records when the first of any of the following events occurs: the material reaches the final stage in the fabrication or manufacturing process; the material is retained for more than 30 days from the date of origination; or the material, regardless of stage of development, is transmitted outside of the facility on a temporary or permanent basis.

- (4) *Incorporation of Classified Material.* When a classified document or other material is joined to, incorporated in or otherwise made a part of another classified document or item of material, accountability for the incorporated document or item of material shall be terminated and accountability for the document or item of material in which it was incorporated shall be established. The control station records shall be posted accordingly. Similarly, when a classified document is disassembled for the purpose of creating a new document or an item of material is removed from a classified assembly or end item (e.g., for testing, replacement), accountability for the new material, if classified, shall be established or adjusted as appropriate in the control station accountability records and the accountability for the basic document or end item shall be terminated provided the residue is unclassified.

g. Dispatch of Classified Material. When classified material is to be dispatched from the facility, the following shall apply:

- (1) The proposed transmittal shall be examined to insure compliance with the preparation for transmission requirements of paragraph 17.
- (2) Receipts, when required by paragraph 17, shall identify the classified contents, the control station, and the

name and address of both sending and receiving facilities. Receipts shall not contain classified information. A short title or abbreviation shall be substituted for a classified title.

- (3) A duplicate copy of the receipt shall be retained in a suspense file until the signed copy is returned. A suspense date (normally not to exceed 30 days) shall be established, and follow-up action shall be initiated if the signed receipt is not received within that period. If after the follow-up action a signed receipt is not returned or the addressee indicates nonreceipt of the classified material, an inquiry shall be conducted in accordance with paragraph 7. Copies of signed receipts for classified material shall be retained at the control station for a minimum of 2 years.

h. Termination of Accountability.

- (1) Upon notice from the cognizant security office that accountability may be terminated for classified material determined to be lost after completion of the inquiries prescribed in paragraph 7, the contractor shall annotate the accountability records to show the date, reason and authority for terminating accountability for the lost material.
- (2) If the location or disposition of the material should subsequently be determined, the contractor shall immediately submit a report to the cognizant security office in accordance with paragraph 6a(15), and shall reestablish accountability for, or indicate correct disposition of, the material on the control station accountability records.

13. Special Requirements for TOP SECRET

- a.* It is mandatory that an up-to-date record be maintained of all persons who are afforded access to TOP SECRET information.

A record shall be maintained which identifies each item of TOP SECRET material, and which shows the names of all individuals given access to the item and the date (or inclusive dates) on which access by each individual occurred. In the case of employees whose duties require knowledge of the combination of containers of TOP SECRET material, the record need only identify the material, the employee(s), and the period of time during which access was available. Such records shall be retained in the appropriate control station for a period of 3 years from the date the material was destroyed, dispatched outside the facility, declassified or downgraded. This record requirement also shall apply to those employees to whom the contractor affords visual or aural access to TOP SECRET information.

b. The number of persons afforded access to TOP SECRET information shall be kept to an absolute minimum, and each person shall be individually warned against disclosing such information to persons whose duties do not require knowledge thereof.

c. The dissemination of TOP SECRET information should be effected orally whenever practicable, without the physical transmittal of material.

d. The transmittal of TOP SECRET material shall be covered by a continuous receipt system both within and outside of the facility.

e. Each copy of a TOP SECRET document shall be numbered in series. The copy number shall be placed on accountability records and on the distribution record and receipt for each TOP SECRET document transmitted.

f. Only designated employees in the control station, cleared for access to TOP SECRET information, shall open incoming TOP SECRET transmittals. Deliveries of TOP SECRET material within the facility shall be accomplished in accordance with paragraph 17f.

g. An annual inventory and accounting of

all TOP SECRET material shall be conducted in the manner prescribed by paragraph 12b.

h. TOP SECRET material shall be reproduced only with the prior written authorization of the contracting officer (see paragraph 18a).

i. Transmission of TOP SECRET material outside of the facility requires the written authorization of the contracting officer (see paragraph 17b).

j. Written approval of the contracting officer is required before disclosing TOP SECRET information to a subcontractor, vendor or supplier (see paragraph 59a).

14. Storage

a. *Containers.* The contractor shall not be eligible to receive, nor have possession of, classified material until he has adequate storage at his cleared facility. Classified material when not in actual use and safeguarded as prescribed in paragraph 16, shall be stored as follows:

- (1) *TOP SECRET—Cabinets and Vaults.* When not in use, TOP SECRET material shall be stored in a security filing cabinet originally procured from an FSS supplier,³ and bearing a GSA Test Certificate Label or in a Class A vault constructed in accordance with the specifications outlined in Appendix IV.⁵

³ Cabinets, contractors, and prices are listed in the FSS (FSC Group 71—Part XI of the GSA, Federal Supply Service). Copies of specifications and schedules may be obtained from any regional office of the GSA.

⁴ Security file cabinets conforming to Federal specifications bear a Test Certification Label on the locking drawer attesting to the security capabilities of the cabinet and lock. Such cabinets manufactured after February 1962 will also be marked "General Services Administration Approved Security Container" on the outside of the top drawer. Acceptable tests of the cabinets shall be performed only by a testing facility specifically approved by GSA.

⁵ When authorized vaults or strongrooms are used for the storage of classified material, bin or shelf storage methods may be employed inside the vault or strongroom. In addition, any type of file cabinet or locking container may be used in the vault or strongroom to provide internal control over dissemination of the classified information.

(2) *TOP SECRET—Supplemental Controls.* In addition to the cabinets and vaults specified in paragraph (1) above, during nonworking hours the following area controls are required:⁶

(a) Entry to the room, building, or structure in which the container is located shall be controlled by a properly cleared, authorized employee or guard stationed so as to control admittance to the room, building or structure, or by a lock which provides reasonable protection against surreptitious entry; and

(b) For the purpose of detecting unauthorized personnel or attempted illegal entry to the container, the interior of the room, building or structure (whichever is controlled in accordance with paragraph (a) above) in which the container is located shall be patrolled and each container inspected at least once during each 2-hour period by a guard, one of whose principal duties is safeguarding classified information, and who is supervised by a system which provides a written record of the coverage of key points within the area; or

⁶ Working hours shall, for purposes of this paragraph, be considered as that period of time when—(i) there is present in the specific area in which a container is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled work shift; and (ii) the number of employees in the scheduled work force is sufficient in number and so positioned as to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude custodians, maintenance personnel and other individuals whose duties require movement throughout the facility.

⁷ The keepers of the steel lock bar shall be secured to the cabinet by welding, rivets, or bolts so that it cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely so that their contents cannot be removed by forcing open the drawer.

(c) The room, building or structure in which the container is located, or the container itself, shall be equipped with an alarm system as prescribed in paragraph 35 and response time to an activated alarm shall not exceed 15 minutes.

(3) *SECRET—Cabinets and Vaults.* When not in use, SECRET material shall be stored in a cabinet or vault authorized for the storage of TOP SECRET or in a security cabinet or vault specified in paragraphs (a) through (g) below.

(a) A filing cabinet originally procured from an FSS supplier and bearing a GSA Test Certification Label.^{3,4}

(b) A Class B vault constructed in accordance with specifications outlined in Appendix IV.⁵

(c) A safe, steel file cabinet or safe-type steel file container having an automatic unit locking mechanism and a built-in three-position, dial-type, changeable combination lock.

(d) A steel file cabinet secured by a steel bar⁷ and a three-position, dial-type, changeable combination padlock, listed on the GSA Qualified Products List as meeting the requirements of Federal Specifications FF-P-110. Non-FSS three-position dial-type changeable combination padlocks in use at the present time may remain in use until replacement is necessary or additional padlocks are required.

(e) A Class C vault constructed in accordance with the specifica-

tions outlined in Appendix IV.⁵

- (f) Other vaults and strongrooms, provided the vault or strongroom is under surveillance by a regularly scheduled hourly guard patrol or is equipped with an alarm system as prescribed in paragraph 35, and the response time to an activated alarm shall not exceed 15 minutes.⁵ (See paragraph F, Appendix IV, for construction criteria.)
 - (g) A steel container in a desk pedestal which encloses the drawer on five sides and is riveted or bolted to the desk, provided the drawer is secured by a steel bar and a three-position, dial-type, changeable combination padlock.⁷
- (4) *SECRET—Supplemental Controls.* In addition to the cabinets and vaults specified in paragraphs (3) (c), (d), (e) and (g) above, during nonworking hours the following area controls are required:⁸
- (a) Entry to the room, building or structure in which the container is located shall be controlled by a properly cleared, authorized employee or guard stationed so as to control admittance to the room, building or structure; or by a lock which provides reasonable protection against surreptitious entry; or by a properly cleared guard stationed at each unsecured perimeter entrance to a complex⁸ which is enclosed by a

physical barrier, and provided further that the area is patrolled adequately to provide reasonable opportunity to detect unauthorized personnel; and

- (b) For the purpose of detecting unauthorized personnel or attempted illegal entry into the room, building, or structure (whichever is controlled in accordance with paragraph (a) above) in which the container is located shall be patrolled at least once during each 4-hour period by a properly cleared, authorized employee (fire patrolman, guard, etc.) one of whose duties is safeguarding classified information and who is supervised by a system which provides a written record of the coverage of key points within the area; or
 - (c) The room, building or structure, in which the container is located; or the container itself, shall be equipped with an alarm system as prescribed in paragraph 35, and the response time to an activated alarm shall not exceed 15 minutes.
- (5) *CONFIDENTIAL—Cabinets and Vaults.* When not in use, CONFIDENTIAL material shall be stored in the same manner as TOP SECRET or SECRET material; however, supplemental controls are not required.

b. *Bulky Material.* When it is impractical to store classified material because of its nature, size or unique characteristics in accordance with paragraph a, above, the contractor shall safeguard such material by control of the area in which it is located, to the extent required by Section IV.

⁸ A complex is a facility or any element thereof which consists of one or more buildings or structures physically enclosed within a common perimeter barrier supplemented by protective measures which prevent unauthorized access and control authorized access.

c. Supervision of Storage Container. Only a minimum number of authorized persons shall possess the combinations to the storage containers or have access to the information stored therein. To facilitate investigation of a container found open and unattended, a record shall be maintained of the names and addresses of persons having knowledge of the combination. Cabinets, vaults and other containers in which classified material is stored shall be kept locked when not under the direct supervision of an authorized person entrusted with the combination or the contents. In the case of one-person facilities, the management official shall inform the cognizant security office of the combination of the container. The combination shall be classified in accordance with paragraph 5i, shall be placed in a sealed envelope marked "to be opened upon death or incapacitation of (name of management official)", and shall be transmitted to the cognizant security office in accordance with paragraph 17. In addition, conspicuously displayed on the outside of the container shall be a notice to contact the cognizant security office prior to opening or moving the container. This notice shall contain the mailing address of and an appropriate telephone number at the cognizant security office. The above provisions pertaining to one-person facilities do not apply to cleared one-person facilities of a multiple facility organization. For such facilities provisions should be made in the home office SPP for affixing an appropriate notice on the outside of the cabinet, and for furnishing the combination to the facility security supervisor of the home office facility who shall be identified as the official to contact rather than the cognizant security office.

d. Protection During Nonworking Hours. Unless specified in a User Agency contract, a contractor shall not be required to establish additional controls over classified material stored in accordance with paragraph a, above.

e. Removal to Residence. Although the contractor may have provided for adequate

storage facilities at the respective residences of his officers, directors, and other employees, removal of classified materials to such dwellings for "after hours" work as a convenience to such persons is not authorized. These facilities, providing they meet the requirements of this Manual, may be utilized for temporary storage purposes only in connection with authorized travel when the individual, in order to accomplish the objectives of the trip, is authorized to carry classified material as prescribed in paragraph 17h, or in other cases of necessity upon approval by an official of the facility who was cleared in connection with the granting of the facility security clearance. In no case will TOP SECRET material be removed to a private residence without (i) the written authorization of the contracting officer in accordance with paragraph 17b, and (ii) approval of the cognizant security office as to the security controls to be maintained over the TOP SECRET material while it remains outside of the facility.

f. Repair of Damaged Security File Cabinets. Neutralization of lockouts or repair of any damage which affects the integrity of a security file cabinet approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance, neutralization of lockouts, and repair of perforations.

- (1) A GSA-approved security file cabinet is considered to have been restored to its original state of security integrity if—
 - (a) All damaged or altered parts (e.g., locking drawer, drawer head, etc.) are replaced with manufacturer's replacement or identical cannibalized parts, or
 - (b) When a container has been drilled immediately adjacent to or through the dial ring to neu-

tralize a lockout, the replacement lock is equal to the original equipment and the drilled hole is repaired with a tapered case-hardened steel rod (e.g., dowel, drill bit, etc.) with a diameter slightly larger than the hole, and of such a length that when driven into the hole there shall remain at each end of the rod a shallow recess of not less than $\frac{1}{8}$ " nor more than $\frac{3}{16}$ " deep to permit the acceptance of substantial welds, and be welded both on the inside and outside surfaces. The outside of the drawerhead shall then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts (e.g., new lock).

- (2) If damage to a GSA-approved or other approved security file cabinet is repaired with welds, rivets, or bolts which cannot be removed and replaced without leaving evidence of entry, the cabinet thereafter may be used for the storage of CONFIDENTIAL material or SECRET material with supplemental controls as outlined in paragraph 14(a)4. If the damage is repaired using methods other than those specified in paragraph (1), above, and herein, use of the cabinet will be limited to unclassified material.

*g. Damage to Approved File Cabinets.*⁴ A list shall be maintained by the facility security supervisor of all approved file cabinets which have sustained damage other than normal marring or scratching from use. Each cabinet listed shall be identified by giving its location and a description of the damage. There shall also be on file a signed and dated certification provided by

the repairer setting forth the method of repair used. The list and certification shall be retained for the life of the file cabinet and shall be available for review during recurring security inspections. Each such cabinet shall have a label posted on the inside of the top drawer to indicate the highest category of classified material which may be stored therein. If the damage affects the integrity of a GSA-approved cabinet, the GSA Approved Security Container label and the GSA Test Certification label shall be removed. However, these labels may be retained by the facility security supervisor for a period of 30 days for those GSA-approved cabinets designated for repair to restore their original integrity. If integrity is not restored within 30 days, the labels shall be destroyed. When a GSA-approved cabinet is repaired in accordance with—

- (1) Paragraph *f(1)(a)*, above, the replacement locking drawer will have its GSA Test Certification label affixed. In this case the retained GSA Approved Security Container label shall be affixed to the outside of the top drawer and the retained GSA Test Certification label shall be destroyed, or
- (2) Paragraph *f(1)(b)*, above, the retained GSA Approved Security Container label shall be affixed to the outside of the top drawer, and the GSA Test Certification label shall be affixed to the inside of the locking drawer.

15. Alternate Storage Locations

a. General. Material classified no higher than SECRET, requiring protection in the interest of national defense and essential to continuity of production operations, may be duplicated and stored in an alternate location, provided the contracting officer approves the use of such storage for information pertaining to the contract. The provisions of Section VI shall apply to the

procurement of this service. Acceptable alternate storage locations are cleared facilities of: (i) a parent, a subsidiary or another facility of a multiple facility organization; (ii) a bank offering safe deposit box/vault facilities; or (iii) a company providing a protective storage service.

b. Security Clearance Requirements. The alternate storage location shall be a cleared facility. Personnel security clearance requirements will depend upon the type of service provided. Where the alternate storage facility is required to provide both secure storage and other services requiring access to the classified information, personnel security clearances are required for employees whose duties will involve access to the classified material or responsibility for providing security protection for the classified material. When the facility is to provide only secure storage space, personnel security clearances are required only for those personnel whose duties involve responsibility for security protection of the classified material.

c. Records. When the alternate storage facility provides both secure storage and file service for the classified information, all of the security requirements prescribed in this Manual shall apply. When the alternate storage facility provides only secure storage service, accountability for the alternate files shall be maintained on a separate record by the facility which deposits the material.

d. Containers. When the services, of a bank are utilized, safe deposit boxes will be considered the equivalent to the FSS security cabinets provided the prime contractor—

(1) Controls the keys to the safe deposit box in the same manner that combinations to storage containers are safeguarded in accordance with paragraph 5i;

(2) Utilizes only cleared employees

whose signatures are on file with the bank to deposit and remove classified material; and

(3) Insures that established procedures preclude access to the classified information by employees of the bank.

16. Safeguards During Use

Classified materials, when not safeguarded as provided for in paragraphs 14a or b, or 34, and when in actual use by authorized personnel, shall be protected as follows:

a. Kept under the constant surveillance of an authorized person, who is in a physical position to exercise direct security controls over the material.

b. Covered, turned face down, placed in storage containers, or otherwise protected, when unauthorized persons are present.

c. Returned to storage containers as soon as practicable after use.

17. Transmission

a. Preparation for Transmission of TOP SECRET, SECRET and CONFIDENTIAL Material.

(1) *Outside of a Facility.* TOP SECRET, SECRET and CONFIDENTIAL material to be transmitted outside of a facility shall be enclosed in opaque inner and outer containers, except as provided for in paragraph (b), (c) or (d) below. If the classified material is printed or written, and is of such size as to permit the use of envelopes for wrapping, the classified information shall be protected from direct contact with the inner container

by a cover sheet or by folding inward. Except as indicated in paragraph (e) below, the inner container shall be addressed, return addressed, carefully sealed and shall be plainly and conspicuously marked with the classification of the contents and, if appropriate, with the notations required by paragraphs 11b(2) and 88a. The outer container shall be addressed, return addressed, and carefully sealed with no marking or notations to indicate that the contents are classified. If the outer container is not sufficiently opaque to prevent the classification markings on the inner cover from being visible, the inner container shall be wrapped with sufficient paper to conceal the markings. If the classified material is of a size, bulk, weight or nature which precludes wrapping as described above, materials used for the packaging shall be of such strength and durability as to provide protection while in transit. To prevent items from breaking out and to facilitate the detection of tampering with the container, the following will be used, whenever practical: seals, kraft paper, kraft tape laminated with asphalt and containing rayon fibers (snake type) or nylon sensitive tape, puncture resistant material; wire mesh or other knife-slash resistant material. As long as the material is enclosed in a double container, the material may be wrapped or boxed in paper, wood, metal, or a combination thereof. When transmitting TOP SECRET and SECRET material the inner container shall contain a receipt form which identifies the addressor, the addressee, and the contents by unclassified or short title. Where this is not practical, the receipt shall be sent to the proposed recipient with

the advance notice of shipment required by paragraphs c(5)(c) and d(3)(d) below, or be handcarried by a responsible employee designated to accompany the classified shipment to its destination. When transmitting CONFIDENTIAL material a receipt form will be enclosed only when the sender deems it necessary. Special provisions for the packaging of classified material are:

- (a) The transmission of written materials of different classifications, for example, the inclusion of CONFIDENTIAL and unclassified with SECRET, in a single package should be avoided. However, when written materials of different classifications are transmitted in one package, they shall be wrapped in a single inner envelope or container, and the receipt required by paragraph (1), above, shall be enclosed. The inner envelope or container shall be marked with the highest classification of its contents.
- (b) If the classified material is an internal component of a packageable item of equipment with an outside shell or body which is not classified and which completely shields the classified aspects of the item from view, the shell or body may be considered as the inner container.
- (c) If the classified material is an inaccessible internal component of a bulky item of equipment that is not reasonably packageable, such as a missile, the outside shell or body of the item may be considered as the

outer container provided the shell or body is not classified.

- (d) If the classified material is an item of equipment that is not reasonably packageable and the shell or body is classified, it shall be draped with an opaque covering that will conceal all classified features. Such coverings must be capable of being secured so as to prevent inadvertent exposure of the item.
- (e) Specialized shipping containers, including closed cargo transporters may be used in lieu of the above packaging requirements. In such cases the container may be considered to constitute the outer container.
- (f) The address may be omitted from the inner and outer container for shipment in full truckload lots, when such an exception is contained in the provisions of the contract. The ASPR requires that complete consignment and marking instructions, to the extent known at the time the contract is awarded, be included in the contract to assist in insuring delivery of items to proper destinations without delay. It further requires that additional consignment instructions be furnished to the contractor as soon as they become known. Under no circumstances will the outer container or the shipping document attached to the outer container reflect the classification of the contents or the fact that the contents are classified.

(2) *Additional Requirements for SECRET Material to be Shipped by Commercial Carrier.*⁹ SECRET material to be transmitted outside a facility by commercial carrier shall be prepared for transmission to afford additional protection against pilferage, theft and/or compromise. Specific provisions for shipment of SECRET material are:

- (a) Except as authorized in paragraph 17a(1), SECRET material shall be shipped in hardened containers (see paragraph 3ah) unless specifically authorized otherwise by the contracting officer or his designated representative.
- (b) The outer container shall be plainly and conspicuously marked, labeled or tagged with the words "Protective Security Service Required" (see paragraph 3ax).
- (c) Carrier equipment shall be sealed by the shipper or at his direction when there is a full carload, a full truckload, exclusive use of the vehicle, or a closed and locked compartment of the carrier's equipment is used. The seals shall be numbered and the number indicated on all copies of the BL. When seals are used, the BL shall be annotated substantially as follows:
DO NOT BREAK SEALS EXCEPT IN CASE OF EMERGENCY OR UPON PRIOR AUTHORITY OF THE CONSIGNOR OR CONSIGNEE. IF FOUND BROKEN OR IF

⁹ Commercial carriers have been issued additional instructions by a separate Supplement which is also applicable to their responsibilities for transmission of SECRET controlled shipments.

BROKEN FOR EMERGENCY REASONS, APPLY CARRIER'S SEALS AS SOON AS POSSIBLE AND IMMEDIATELY NOTIFY BOTH THE CONSIGNOR AND THE CONSIGNEE.

- (d) The notation "Protective Security Service Required"¹⁰ shall be reflected on all copies of the BL. The BLs will be maintained in a suspense file to follow up on overdue or delayed shipments.

- (3) *Within a Facility.* TOP SECRET, SECRET and CONFIDENTIAL material shall be prepared for transmission within a facility in such manner as to insure a degree of security protection adequate for the method of transmission to be used, using guidance contained in paragraph (1) above. Double covering of the material is not required for intraplant transmission. However, in all cases, adequate measures shall be taken to protect against unauthorized disclosure of classified information.

b. Method of Transmission of TOP SECRET Material Outside a Facility. When a contractor is authorized in writing, by the contracting officer or his designated representative, TOP SECRET material may be transmitted by: (i) specifically designated escort or courier cleared for access to TOP SECRET information (military, U.S. civilian employee, or a responsible employee designated by the contractor, except that the contractor employee shall not carry classified material across international boundaries); (ii) Armed Forces Courier Service

in accordance with the instructions of the contracting officer, (iii) by electrical means in a CRYPTO system approved for encryption of TOP SECRET information. Under no circumstances shall TOP SECRET material be transmitted through the U.S. or company mail channels.

c. Method of Transmission of SECRET Material Outside a Facility. SECRET material shall be transmitted by one of the following means within and between the U.S., Puerto Rico, Panama Canal Zone or a U.S. possession or trust territory:

- (1) One of the means established for TOP SECRET.
- (2) By U.S. Registered Mail, including U.S. Registered Airmail, through U.S. civil postal facilities or Army, Navy or Air Force postal facilities. However, U.S. Registered Mail destined for activities located in the Panama Canal Zone must be routed only via the military postal system. Addresses may be obtained from the DoD Activity Address Directory, DoD 4000.25-D (a reference copy is located at the cognizant security office), or from the ACO/PCO. A copy of DoD 4000.25-D may also be purchased from the GPO.
- (3) Appropriately cleared employees of the contractor, who have been designated and briefed in their responsibilities as couriers or escorts for protecting the SECRET material. When such couriers or escorts are utilized, the classified material remains under the constant custody and protection of the contractor personnel at all times and the commercial transportation service (ship, rail, air or truck) is not required to have a facility security clearance. Escorts or couriers shall always accompany shipments when

¹⁰ In such cases the SECRET shipment shall be routed via a cleared commercial carrier under a tariff, tender or contract that provides Protective Security Service in accordance with the Carrier Supplement to this Manual.

rail or ship transportation is involved (see Appendix X for use of escorts for classified shipments and Appendix XI for hand carrying of classified documents aboard commercial passenger aircraft).

- (4) By electrical means over approved CRYPTOGRAPHIC communication circuits (telephone, wire, radio or an intercommunication system), including computer data, but only with the prior written approval and in accordance with the instructions of the contracting officer.
- (5) By commercial carriers¹¹ (air or surface) *only* when the size, bulk, weight, nature of the shipment, shipping costs or escort considerations make the use of the foregoing methods impractical. Only qualified carriers (see paragraph 3ay) will be used for the transmission of SECRET material. When the services of a commercial carrier are required, the contractor, as consignor shall:
 - (a) Utilize a qualified carrier selected by the Government that will provide a single line service from point of origin to destination, when such service is available, or by such transshipping procedures as may be specified by the Government, and
 - (b) Request routing instructions, including designation of a qualified carrier, from the contracting officer or designated representative (normally the Government transportation officer). The request shall speci-

fy that the routing instructions are required for the shipment of SECRET material via Protective Security Service (Do Not Abbreviate) and include the point of origin and point of destination, or

- (c) As an exception to the general requirements enunciated above, if time is of the essence and the total shipment weighs less than 200 pounds gross, the contractor, as consignor, may make arrangements directly with a cleared commercial carrier to provide Protective Security Service for the transporting of the SECRET shipment when a CBL is to be used. This exception may not be utilized for COMSEC or SENSITIVE COMPARTMENTED INFORMATION material without the approval of the PCO. Under this exception the contractor must specify to the commercial carrier that SECRET material is to be shipped and that Protective Security Service is required. The points of origin and destination must also be provided. Verification of the clearance of the commercial carrier and the fact that it provides Protective Security Service is to be obtained from the cognizant security office of the home office of the carrier prior to release of any classified material, and
- (d) Notify the consignee (including Government transshipping activity) of the nature of the shipment, the means of shipment, numbers of the seals, if used, and the anticipated time and date of arrival by separate communication at

¹¹ Commercial carriers may be used only within and between the 48 contiguous States and the District of Columbia or wholly within Alaska, Hawaii, Puerto Rico, Panama Canal Zone or a U.S. possession or trust territory.

least 24 hours in advance, (or immediately upon dispatch if transit time is less than 24 hours) of the arrival of the shipment, in order that the consignee may take appropriate steps to receive and protect the shipment. Request the consignee (including a military transshipping activity) to notify the consignor of any shipment not received within 48 hours after the estimated time of arrival indicated by the consignor. In addition, the consignor shall annotate the BL to require the carrier to provide immediate notice to the consignor of any delay en route, regardless of the reason of delay. Upon receipt of either the consignor immediately shall request the carrier to trace the shipment and shall notify his cognizant security office in accordance with paragraph 6a (10) of the delay in the delivery of the classified material and the circumstances as known to the consignor. Subsequent developments concerning the delayed shipment shall also be reported to the cognizant security office. A copy of the report shall also be submitted to the contracting officer concerned or his designated representative. The consignee, consignor and carrier are required to take similar inquiry and reporting action if a shipment is received with broken seals or the numbers on the seals do not match those on the advance notice of shipment.

- (6) By such other methods directed through specific instructions from the contracting officer or his designated representative because of spe-

cial considerations or the nature of the shipment (e.g., explosives, high priority items, nuclear weapons or direct shipments between military installations).¹²

*d. Method of Transmission of CONFIDENTIAL Material Outside a Facility.*¹² Such material shall be transmitted by one of the following means within and between the U.S., Puerto Rico, Panama Canal Zone or a U.S. possession or trust territory:

- (1) One of the means established for SECRET in paragraphs c(1), (2), (3), (4) and (6) above.¹¹
- (2) U.S. Express Mail¹³ or U.S. Certified Mail for CONFIDENTIAL material. However, U.S. Registered Mail shall be used for transmittal of such material between any of the following points: the CONUS, Alaska, Hawaii, Puerto Rico, Panama Canal Zone, or a U.S. possession or trust territory. In addition, U.S. Registered Mail destined for and between activities located in the Panama Canal Zone must be routed only via Army, Navy or Air Force postal facilities. Addresses may be obtained from the DoD Activity Address Directory, DoD 4000.25-D (a reference copy is located at the cognizant security office), or from the ACO/PCO. A copy of the DoD 4000.25-D may be purchased from the GPO.
- (3) By commercial carrier¹¹ (air or surface) *only* when the size, bulk, weight,

¹² When a shipment by truck is contemplated for classified CM (CONFIDENTIAL or SECRET), the contracting officer will issue specific shipping instructions requiring a driver holding a final SECRET clearance in addition to the military escort normally provided for such shipments.

¹³ U.S. Express Mail is a premium mail service consisting of both programmed and regular service. The service is intended for, but not limited to, use by the business mailer or other large volume user of the mails. The service is a high-speed intercity delivery system that usually can negate the requirement to hand carry CONFIDENTIAL material in cases of short notice. Additional information is available through a local postal Customer Service Representative regarding the specific options which are available.

nature of the shipment, shipping costs or escort considerations make the use of the foregoing methods impractical. The commercial carrier must be authorized by law, regulatory body or regulation to provide the required transportation service and a determination must be made by MTMC that the carrier has a tariff, Government tender, agreement or contract which provides a Signature Security Service. A facility security clearance is not a requirement. The foregoing information may be obtained from the contracting officer or his designated representative. In addition to the aforementioned coordination with the contracting officer or his designated representative, the contractor, as consignor shall:

- (a) Utilize containers of such strength and durability as to provide security protection to prevent items from breaking out of the container and to facilitate the detection of any tampering with the container while in transit.
- (b) Indicate on the BL "Signature Security Service Required." In addition, the consignor shall annotate the BL to require the carrier to notify the consignor immediately if the shipment is delayed en route for any reason.
- (c) Instruct the carrier to ship packages weighing less than 200 pounds gross in a closed vehicle or a closed portion of the carrier's equipment.
- (d) Notify the consignee (including a Government transshipping activity) of the nature of the shipment, the means of shipment and the anticipated date and time of arrival, by separate communica-

tion at least 24 hours in advance (or immediately upon dispatch if transit time is less than 24 hours) of the arrival of the shipment in order that the consignee may take appropriate steps to receive and protect the shipment. Request the consignee (including a military transshipping activity) to notify the consignor of any shipment not received within 48 hours after the estimated time of arrival indicated by the consignor. Upon receipt of such notice, the consignor immediately shall request the carrier to trace the shipment and shall notify his cognizant security office in accordance with paragraph 6a(10) of the delay in the delivery of the classified material and the circumstances as known to the consignor. Subsequent developments concerning the delayed shipment shall also be reported to the cognizant security office. A copy of the report shall also be submitted to the contracting officer concerned or his designated representative for forwarding to MTMC.

e. Method of Transmission of SECRET and CONFIDENTIAL Material Outside of Areas Enumerated in Paragraphs 17c and d SECRET and CONFIDENTIAL material shall be transmitted only under the provisions of the contract or with the written authorization of the contracting officer. However, when the classified material had previously been authorized for export under a State Department license or letter, the contractor shall notify the contracting officer of the classified material to be transmitted outside of the areas enumerated in paragraphs c, and d, above. A contractor shall not transmit classified material directly to a foreign government or firm. The only exception to this would be when a foreign government, with whom the U.S. has entered into

a reciprocal agreement pertaining to the filing of classified patent applications in the respective countries, has authorized its U.S. patent agent to return its foreign classified information directly to that foreign government. Except as noted above, transmission shall take place between the contractor and a designated U.S. Government representative for forwarding to the foreign activity. This is known as transmission by government-to-government channels. Transmittal arrangements shall be made by the cognizant security office where the foreign firm or government has awarded a contract to the U.S. contractor. When authorized, SECRET and CONFIDENTIAL material shall be transmitted by one of the following means.

- (1) Accompanied by a contractor employee courier or escort, who is cleared for access to the classified information involved and who has been designated by the contractor, provided:
 - (i) the classified material is not transported across international borders (this does not preclude use of regularly scheduled non-stop flights on U.S. carriers between the U.S. mainland and Alaska, Hawaii, Puerto Rico, the Panama Canal Zone, or U.S. possessions or trust territories), (ii) time limitations do not permit the use of U.S. Government channels, (iii) an appropriate courier or escort authorization is issued to the employee, (iv) the transmission is begun and completed during normal daytime duty hours of the same day and is by surface means only and within the national borders of the country within which the transmission takes place, and (v) the employee can comply with the specific security instructions for the safeguarding of classified material involved; i.e., storage at a U.S. Government installation within the country concerned.
- (2) Accompanied by a U.S. Government Civil Service employee or military person who is cleared for access to

the level of the classified information involved and who has been designated by the contracting officer. (Appropriately cleared officers of the Department of Navy, Military Sea Transportation Service Civilian Marine Personnel, may also be designated as escorts by the contracting officer.) Foreign carriers may not be utilized, unless the designated escort has continuous physical control of the material being transported.

- (3) Registered mail through U.S. Army, Navy or Air Force postal facilities. If the intended recipient is not authorized to receive classified material through APO channels, arrangements shall be made with an activity which is so authorized to receive and hold the classified material pending pick-up by the intended recipient.
- (4) U.S. and Canadian registered mail with registered mail receipt to and from Canada in accordance with instructions from the contracting officer and via a U.S. or Canadian Government activity.
- (5) Armed Forces Courier Service in accordance with specific instructions from the contracting officer.
- (6) In accordance with specific instructions from the contracting officer whenever the nature of the classified shipment does not lend itself to transmission by any of the above methods. In such cases the procedure for advance notice to consignee and reporting of delayed receipt, etc., set forth in paragraph c(5)(c) above, apply.

f. Method of Transmission of TOP SECRET, SECRET and CONFIDENTIAL Material Within a Facility. Shall be transmitted within a facility by a responsible employee designated by the contractor, and who has been cleared for access to the category

of classified information involved. The classified material shall remain under the direct surveillance of the designated employee at all times. By electrical means over approved CRYPTOGRAPHIC communication circuits with the prior written approval and in accordance with instructions of the contracting officer, or other approved circuits with the prior written approval of the cognizant security office.

g. Inspection of Classified Shipment. Upon receipt of a classified shipment the consignee shall examine it to insure that there is no evidence of tampering (see paragraph 12e(2)). Evidence of tampering shall be reported to the cognizant security office in accordance with paragraph 6a(11).

h. Protection En Route by Contractor's Employee. When employees designated by the contractor are used to transmit or carry classified material, the storage provisions of paragraph 14 shall apply at all stops enroute to destination, unless the material is retained in the personal possession of the employee at all times. This involves constant surveillance by the employee who is in a physical position to exercise direct security controls over the material at all times. The hand carrying of classified material on trips that involve an overnight stopover is not permissible unless arrangements are made in advance of departure for overnight storage of the hand-carried classified material in a Government installation or a cleared contractor's facility. Transmission or carrying of classified material shall not be authorized when there is doubt as to whether the material can be properly handled and protected. Additional special requirements for hand carrying of envelopes containing classified documents aboard commercial passenger aircraft are contained in Appendix XI. These procedures however, apply to classified documents only. Instructions for hand carrying classified hardware and other bulky packages aboard commercial passenger aircraft shall be obtained from the cognizant security office on a case-by-case basis.

i. Additional Protection in Connection With Visits. When classified material, other than TOP SECRET, is required on a visit, such material shall be addressed by the contractor to his employee making the visit and shall be transmitted to the destination being visited, to be held for the employee, in accordance with paragraph c(2) or d(2) above. This method also shall be used for the return of the material. However, if the contractor determines that time limitations do not permit mailing the material required during the visit, he may authorize the employee concerned to carry the classified material subject to the provisions of paragraph h, above. An inventory of the material shall be made prior to departure and retained at the control station. A copy of the inventory shall be carried by the employee. Only that classified material absolutely essential to the purpose of the visit may be carried by the employee. Upon the employee's return from the visit, an inventory shall be made of the material for which he is charged. If, in connection with the purpose of the visit, classified material is not returned to the facility, a receipt shall be obtained and the transaction shall be recorded in the records of the control station in accordance with paragraph 12.

j. COMSEC Information. Classified COMSEC information shall be transmitted as prescribed in the COMSEC Supplement to this Manual.

k. Addressing Mail or Shipments of Classified Material. Except as provided below, mail or shipments containing classified material shall be addressed to the Commander or Head of the User Agency activity or installation (Commander, Commanding Officer, Director, or similar designation) or to the cleared facility concerned, using the appropriate business name and address, and not to an individual. This does not prevent use of office code letters or numbers, or such phrases in the address as, "ATTN: Research Dept." or similar aids in expediting internal

routing in addition to the appropriate address.

- (1) When it is considered desirable or appropriate to direct SECRET or CONFIDENTIAL material to the attention of a particular employee of a facility or User Agency, other than to a consultant as prescribed below, the identity of the intended recipient shall be indicated on an attention line on the inner container or on an attention line placed in the letter of transmittal. If such mail is to be delivered directly to the specified employee, a procedure shall be established to insure that all classified enclosures are promptly entered into the facility's document control system in accordance with paragraph 12.

- (2) When transmitting SECRET or CONFIDENTIAL material to an individual operating as a cleared facility or engaged as a Type B or C consultant, or to any facility at which only one employee is assigned, the contractor shall specify on the outer container "TO BE OPENED BY ADDRESSEE ONLY." Further, the outer container shall be annotated "Postmaster—Do Not Forward. If Undeliverable to Addressee, Return to Sender." Although postal regulations allow "Restricted Delivery" mail to be delivered to the addressee or to an agent the addressee has authorized in writing to receive his/her "Restricted Delivery" mail, in all instances only appropriately cleared personnel shall be designated as agents for the addressee. Additionally, in the event the consultant is operating as a Type C consultant, arrangements shall be made by the consultant to insure that all incoming U.S. Certified Mail, U.S. Registered Mail, and U.S. Express Mail addressed to him in his capacity as an independent consultant is delivered

unopened to him personally through his employer's mail distribution system before entering it into his employer's document control system.

1. RESTRICTED DATA and FORMERLY RESTRICTED DATA. RESTRICTED DATA and FORMERLY RESTRICTED DATA shall not be transmitted or otherwise made available to any regional defense organization or foreign government, except under the provisions of the Atomic Energy Act of 1954, as amended, and in accordance with instructions issued by the contracting officer concerned.

18. Reproduction

All copies of reproductions of classified material shall be marked or stamped with the same classification as the original. Only sufficient copies necessary to meet operational requirements shall be prepared, and reproductions shall be destroyed, if otherwise proper, as soon as they have served their purpose. Reproduction of classified material shall be made only on equipment specifically designated for the reproduction of classified material. Rules governing the use of such designated equipment will be conspicuously posted on or near the equipment. Further, appropriate warning notices prohibiting reproduction of classified material shall be posted on or near equipment used only for the reproduction of unclassified material.

a. Reproduction by Authorization Only. The contractor shall not make nor permit to be made without prior written authorization of the contracting officer, or his designated representative, any photograph or other reproduction of TOP SECRET information, SECRET information (when specifically prohibited), or CRYPTO information, regardless of classification, for any purpose. However, if the contract is for a TOP SECRET, SECRET or CRYPTO report, then additional reproduction authority

is not necessary. (See paragraph 87a regarding restrictions on the reproduction of COSMIC TOP SECRET information.) In addition, TOP SECRET and SECRET material originated by the ERDA or its contractors may be reproduced only with the consent of the originator or higher authority within the responsible ERDA activity.

b. Reproduction Not Requiring Authorization. The contractor may reproduce, without prior authorization of the contracting officer, non-CRYPTO information classified SECRET (unless specifically prohibited) or CONFIDENTIAL when such reproduction is essential to—

- (1) The performance of the contract.
- (2) The preparation of a solicited or unsolicited bid, quotation, or proposal to a User Agency of the U.S. Government or another authorized contractor for U.S. Government work.
- (3) Correspondence in connection with the contract.
- (4) Preparation of patent application to be filed in the U.S. Patent Office. (This paragraph shall not be deemed to authorize the filing of patent applications, and such applications shall not be filed except as specifically provided in the contract.)

c. Records. The contractor shall maintain a record of the number of copies of all TOP SECRET and SECRET material, and CRYPTO material, regardless of classification, that he reproduces. Reproduction records shall be retained by the contractor, for a minimum of 3 years for TOP SECRET, CRYPTO or other Special Access material and for a minimum of 2 years for SECRET, and shall be incorporated in the control station records required by paragraph 12.

d. Additional Markings. When reproducing classified material, the additional notations required by paragraph 11b shall be shown on all reproductions.

19. Destruction

a. Requirement for Destruction. The contractor shall establish a program for the review of classified material for the purpose of reducing to an absolute minimum the quantity on hand at any given time. With the exception of information listed in paragraph b, below, the contractor shall destroy classified material in his possession as soon as practicable after it has served the purpose for which it was—

- (1) Released by the Government.
- (2) Developed or prepared by the contractor.
- (3) Retained after completion or termination of the contract.

b. Disposition by Specific Authorization. COSMIC TOP SECRET material (see paragraph 85c(2)) shall not be destroyed but shall be returned to the contracting officer or his designated representative. Accountable COMSEC classified material shall be destroyed only when destruction is authorized in writing by an appropriate Government official. In all instances where specific instructions have been issued by the contracting officer, such instructions will dictate the disposition to be accomplished.

c. Methods of Destruction. Classified material shall be destroyed beyond recognition so as to preclude reconstruction of the classified information in whole or in part. The destruction, which may be limited to those components or portions of the material which incorporate classified information, can be accomplished by burning, melting, mutilation, or chemical decomposition. In addition, pulping, disintegration, pulverizing, or shredding may be used for the destruction of paper products. Methods of destruction, other than burning, and the equipment used for such, shall be approved by the cognizant security office. Public incinerators may be used only with the prior approval of, and under conditions prescribed by the cognizant security office. The following additional requirements pertain to destruction:

- (1) If classified material is removed from the facility for destruction, it shall be destroyed on the same day it is removed.
- (2) The equipment and methods used to destroy classified material shall be inspected each time destruction is effected to assure that the minimum requirements approved by the cognizant security office are met.
- (3) When classified paper products are shredded, the residue shall not exceed a size greater than 1/32" in width (with a permissible plus tolerance of 1/64") by 1/2" in length, and shall be accomplished in sufficient quantities of material, and types of paper, to preclude reconstruction or recognition of the material being destroyed. Shredding is not authorized for the destruction of TOP SECRET.
- (4) The SPP shall include specific instructions which apply to the method of destruction, and shall incorporate instructions provided by the cognizant security office.

d. Witness to Destruction. The destruction of classified material shall be accomplished by or in the presence of two employees of the contractor who possess appropriate security clearances. One shall be a responsible employee who has been briefed in the destruction provisions of this paragraph, and who has been designated by the contractor to perform the destruction. The other shall be a responsible employee or a

subcontract employee who is working on the premises of the contractor and who has been designated to witness the destruction of the classified material. However, CONFIDENTIAL material, other than accountable COMSEC material, may be destroyed at the facility and witnessed by: (i) one responsible employee or (ii) one responsible subcontractor guard who is employed on a full-time basis at the facility, is under the supervision and direction of the facility security supervisor and possesses an appropriate security clearance, has been briefed in the destruction procedures, and has been designated to perform and witness the destruction.

e. Destruction Records and Certificates for TOP SECRET, SECRET or CRYPTO Material. When TOP SECRET, SECRET, or CRYPTO material, regardless of classification, is destroyed the contractor, in addition to maintaining accountability records reflecting the destruction of such material, shall execute a destruction certificate indicating the date of destruction and identifying the material destroyed. The certificate shall be signed by both the individual designated to destroy and the individual designated as a witness at the time the material is destroyed. Both individuals shall be required to know, through their personal knowledge, that such material was destroyed. The contractor may, at his discretion, combine the information required in the destruction certificate with the accountability records maintained in accordance with paragraph 12a. Upon request, a copy of the destruction certificate shall be sent to the contracting officer at the time of destruction.

Destruction records and destruction certificates shall be maintained at the control stations established under paragraph 12, and shall be retained by the contractor for a minimum of three years for TOP SECRET, Special Access, or CRYPTO material, regardless of classification, and for two years for SECRET material.

f. Classified Waste. Classified waste shall be destroyed as soon as practicable in accordance with the provisions of paragraph *c*, above. This applies to all waste material containing classified information, such as preliminary drafts, carbon sheets, carbon ribbons, plates, stencils, masters, stenographic notes, worksheets and similar items. (Typewriter and automatic data processing equipment ribbons used in transcribing classified material shall be safeguarded in the manner appropriate for the classification category involved until the ribbon is cycled through the typewriter or printer a sufficient number of times to obliterate information contained thereon. Normally this can be accomplished if the ribbon is completely overprinted five times in all ribbon typing or printing positions. Any ribbon which remains substantially stationary until it has received at least five consecutive impressions shall be treated as unclassified.) CONFIDENTIAL waste, except waste containing CRYPTO or other Special Access information, may be destroyed by one employee or one responsible subcontractor guard pursuant to the provisions of paragraph *d*, above. Pending destruction, classified waste shall be safeguarded in accordance with paragraph 14. Receptacles utilized to accumulate classified waste shall be clearly identified. If not promptly destroyed, accountability shall be established over that material containing information classified SECRET or higher and CRYPTO or Special Access information regardless of classification, in accordance with paragraph 12*f*. When destruction does take place, the provisions of paragraph *e*., above are applicable.

g. Alternate Procedure. Where there is

only one employee assigned at a facility and there is a need to destroy classified material, one or more of the following alternate procedures shall be used for disposal of the classified material:

- (1) Return all classified material eligible for destruction, including classified waste, to the contractor or User Agency for whom the classified work is being performed, or to another facility of the same multiple facility organization.
- (2) Utilize the destruction facilities of another DoD contractor or User Agency, provided that the individual granted use of such facilities retains physical custody of the classified material and personally insures its complete destruction. To satisfy the requirements of paragraphs *d*, and *e*, above, an appropriately cleared employee of the contractor or User Agency providing the destruction service may serve as a witness to the destruction and sign the destruction certificate.
- (3) Employ the destruction services of a subcontractor, vendor or supplier specializing in the destruction of classified material, provided that the controls set forth in paragraph *c*, above are observed, and an appropriately cleared employee of another DoD contractor or User Agency is present to witness the destruction when required pursuant to paragraph *d*, and *e*, above.

h. Magnetic Recordings.

- (1) All classified information recorded on magnetic media shall be safeguarded and accounted for according to the requirements prescribed in this Manual for the highest level of classified information ever recorded thereon.

DoD 5220.22-M

- (2) When the classified information re-recorded on magnetic media is itself regraded or declassified, the recording media shall be regraded in accordance with the provisions of paragraph 11c and, except when completely declassified, safeguarded according to the requirements prescribed in this Manual for the new level of classification.
- (3) Procedures for declassification of magnetic recording media are located in paragraph 107.

SECTION III

SECURITY CLEARANCES

20. General

a. An individual shall be permitted to have access to classified information only when cleared by the Government or by the contractor as specified in this Section; and when the contractor determines that access is necessary in the performance of tasks or services essential to the fulfillment of a contract or program, i.e., the individual has a need-to-know (see paragraph 3as). The contractor shall limit the number of personnel processed for clearance to the maximum extent possible consistent with contractual obligations.

b. To be eligible for a personnel security clearance, the following age must have been attained.

	<i>Years</i>
For CONFIDENTIAL	16
For SECRET or TOP SECRET	18

c. A security clearance granted by the DoD, or by a contractor as specified in this Section, is valid for access on a need-to-know basis to all classified defense information at the same or lower category, except that: (i) contractor CONFIDENTIAL clearances are not valid for access to RESTRICTED DATA; COMSEC information (see paragraph 76); SENSITIVE COMPARTMENTED INFORMATION (see paragraph 75); ACDA classified information; NATO information (see paragraphs 85 and 86 (a contractor CONFIDENTIAL clearance is valid, however, for access to NATO RESTRICTED information only) or, to meet the security clearance requirement as a prior condition for certification to fill a Critical or Controlled Position under the Nuclear Weapon PRP (see paragraph 3at.1); (ii) interim SECRET

or interim CONFIDENTIAL clearances are not valid for access to RESTRICTED DATA, NATO, or COMSEC and SENSITIVE COMPARTMENTED INFORMATION (interim TOP SECRET clearances are, however, valid for access to RESTRICTED DATA, NATO, COMSEC, and SENSITIVE COMPARTMENTED INFORMATION only at the SECRET category and below; (iii) access under Canadian and U.K. Reciprocal clearances is limited as set forth in paragraph 31d; (iv) clearances issued to immigrant aliens are not valid for access to NATO classified information, COMSEC information or SENSITIVE COMPARTMENTED INFORMATION. In addition to a final security clearance granted by the DoD, a CRYPTOGRAPHIC Access Authorization is required for access to CRYPTO information; and the specific authorization of the User Agency is required for access to SENSITIVE COMPARTMENTED INFORMATION.

d. Personnel shall not be cleared for access to classified information of a higher level than the clearance of the facility at which they are employed, except for—

- (1) Type A Consultants, as provided in paragraph 68.
- (2) Employees of a multiple facility organization who are physically located at an uncleared facility or a facility with a lower level of clearance, who require access to a higher category of classified information exclusively in connection with the performance of duties at another cleared facility or at a Government installation; or who are transferred to an uncleared facility or to a facility with a lower level

of clearance within the multiple facility organization, provided the contractor desires to retain the Letter of Consent at the higher level so it will be available in the event the individual is transferred back to a facility at which the clearance will be needed. A clearance granted under this authority shall not be of a higher level than the facility clearance of the home office of the contractor, and the Letter of Consent will be issued or forwarded to the HOF or to the PMF, as appropriate. If the contractor elects to have the Letter of Consent retained at a PMF in accordance with paragraph 26*k*, clearances granted to personnel located within the geographical or functional area of responsibility assigned to the PMF shall not be of a level higher than the facility clearance of the PMF.

e. All personnel assigned the duty or entrusted with the responsibility of safeguarding classified material shall be cleared at the same level as the facility at which they are assigned, except that such personnel will be required to have a TOP SECRET clearance only if the person's duties require that he have access to or possession of TOP SECRET information, or is exercising control over TOP SECRET areas as prescribed by paragraph 34. This rule shall apply to those personnel whose duties involve the safeguarding of classified material whether they are: acting as guards in addition to other regularly assigned functions (guards required by paragraph 34 shall not be assigned additional functions which will interfere with their protective duties); employed by the contractor for the primary purpose of serving as a member of the police, guard, or protective force of the facility; or employees of a firm awarded a contract to furnish police, guard, or protective services at the cleared facility.

f. The fact that a contractor has qualified

for and has been granted a facility security clearance shall not be used for advertising, promotional purposes or in the recruitment of employees. Employment advertisements shall not state or imply that a personnel security clearance is a condition or prerequisite for employment. Reproduction in any manner of the DLA Form 381-R, furnished to the contractor by the Government, shall not be made except for the necessary records of the contractor or unless requested by competent Government authority. Further, the reproduction in any manner of a Letter of Consent or Security Assurance furnished by the Government to the contractor for his employee shall not be made except for necessary records of the contractor, unless requested by competent Government authority. A copy of the Letter of Consent or Security Assurance shall not be furnished the employee named on the form for any purpose whatsoever, nor shall the employee be given any other written notification of the granting of a Letter of Consent or Security Assurance. However, this does not preclude the issuance of a color-coded identification card or badge to reflect the level of clearance in accordance with paragraph 8.

g. When DISCO determines that it is unable to obtain the full investigative requirements to meet prescribed standards for the level of clearance requested, the contractor shall be advised that such clearance cannot be granted because of such inability, and the clearance action shall be discontinued.

h. Unless administratively terminated, suspended or revoked by the DoD, the clearance of an employee shall be effective so long as he is continuously employed by the contractor, and during any period of reemployment by the contractor which commences within 12 months after the cessation of prior period of employment provided DISCO is notified of the reemployment in accordance with paragraph 6*b*(2). However, if the employee no longer has or requires access to classified information and no requirement

for such access is anticipated in the foreseeable future, clearance can be administratively terminated by complying with paragraph 29. In addition, when an employee is granted a leave of absence, it shall not be considered as an interruption or discontinuance of employment provided it does not exceed 1 year. When the leave of absence granted the employee exceeds 1 year, the termination date reported in accordance with paragraph 6b(2) will be the first day of the leave of absence.

i. In all cases in which a contractor furnishes copies of board minutes, certificates, or other records, such records shall be on company letterhead or identified by typing the contractor's name and address and, in addition, they shall indicate the date of submission.

j. As a general rule a contractor may be issued only one Letter of Consent for each cleared employee. However, in the case of an individual who, pursuant to paragraph 22, is required to be cleared in connection with the home office facility clearance and who has his primary place of work at another facility of the multiple facility organization, a Letter of Consent may be issued to both facilities.

k. Requests for clearance of personnel required to be cleared in connection with a facility security clearance as prescribed by paragraph 22, who are also representatives of a foreign interest, shall be submitted to the cognizant security office. All other requests for clearance of employees who are representatives of a foreign interest shall be submitted to DISCO. A representative of a foreign interest (see paragraph 3bb) is not eligible for a personnel security clearance if:

- (1) The foreign interest involves a Communist country or a citizen, firm, or other entity of a Communist country; or

- (2) The individual's work as a representative of a foreign interest could create a potential conflict of interest situation vis-a-vis his work for the contractor if a personnel security clearance were to be issued on his behalf. (A potential conflict of interest situation is considered to exist where an individual's technical or scientific endeavors on behalf of a foreign interest are similar to his technical or scientific endeavors on behalf of the U.S. contractor, i.e., the individual is performing services as a consultant to a foreign government and to a contractor involving the same general scientific or technical discipline.)

- (3) The individual is not a U.S. citizen or U.S. national. This general exclusion is not applicable to Canadian or U.K. citizens who are eligible for or have been previously granted a Reciprocal clearance in accordance with the provisions of paragraph 31.

Decisions as to whether an individual is eligible for a personnel security clearance pursuant to paragraph (1), (2) or (3) above, are made by DLA. With the exception of the foregoing, a representative of a foreign interest is eligible for consideration for a personnel security clearance provided he submits a statement explaining fully his foreign connections. The statement should identify the foreign entity. If it is a business enterprise, the statement should include explanation as to the nature of the business and to the extent possible, details as to its ownership, including the citizenship of the principal owners or blocks of owners. The statement should fully explain the nature of the relationship between applicant and the foreign entity and indicate the approximate percentage of the applicant's time devoted to the interest of the foreign entity. In addition, the statement shall incorporate the provision that the applicant recognizes

DoD 5220.22-M

his special responsibility to protect classified information from disclosure to any unauthorized person, foreign or domestic. Two copies of the statement described above shall be included with each request for an initial clearance, transfer of clearance, concurrent clearance or conversion of clearance. In those cases where an individual who is cleared (or is in the process of being cleared) becomes a representative of a foreign interest, the contractor shall submit a written report in accordance with either paragraph 6a(4) or 6b(5). This report shall include the statement described above. In those cases where a representative of a foreign interest is required to be cleared in connection with a facility security clearance pursuant to paragraph 22, the provisions of paragraph 22f are applicable, in addition to the provisions of this paragraph.

l. Foreign nationals are not eligible for a personnel security clearance, except that reciprocal clearances may be granted to citizens of Canada and the U.K. in accordance with paragraph 31.

m. Except for short-term visits (not in excess of 90 consecutive days during any 12-month period) residence or the assignment of a cleared immigrant alien outside the U.S., (Puerto Rico, Guam or the Virgin Islands) negates the basis upon which the Letter of Consent was issued, and the Letter of Consent shall be administratively terminated without prejudice by DISCO upon receipt of notification of such residence or assignment (see paragraph 6b(6)).

n. Persons not eligible for clearance under the provisions of this Section shall be granted access to classified information only as specially authorized in writing by a User Agency. The granting of such access is beyond the scope of the Industrial Security Program and all necessary instructions will be provided by the User Agency concerned.

o. When an interim personnel clearance

has been granted and derogatory information is subsequently developed, DISCO may withdraw the interim clearance pending completion of the processing which is a prerequisite to the issuance of a final clearance. When an interim personnel clearance for an individual who is required to be cleared in connection with the facility security clearance pursuant to paragraph 22 is withdrawn, the interim facility clearance will also be withdrawn unless action is taken to remove the individual from the position requiring clearance. Withdrawal action is not a denial or revocation of clearance and is not appealable.

21. Facility Security Clearances

a. *Procedures for Processing.* A facility security clearance is an administrative determination that a facility (see paragraph 3ab) is eligible from a security viewpoint for access to classified information of the same or lower classification category as the clearance being granted. Facility security clearances shall not be granted to contractor activities located outside the U.S., Puerto Rico, Panama Canal Zone, or a U.S. possession or trust territory. Facility clearances may be granted only to contractors organized and existing under the laws of any of the United States and Puerto Rico. Contractors organized and existing under the laws of the Panama Canal Zone or a U.S. possession or trust territory may not be processed for or granted a clearance unless prior approval is received from DLA-DD (CAS). The cognizant security office assigned responsibility for the geographic area in which the facility is located (See Appendix VIII) will advise the prospective contractor of the actions required for the processing, the issuance and the continuation of a facility clearance. In connection with the issuance of a facility clearance, personnel security clearances must be granted to certain management personnel as prescribed in paragraph 22. In addition, the contractor shall execute a DD Form 441, or, where ap-

appropriate, an Appendage to Department of Defense Security Agreement DD Form 441—1) and a Certificate Pertaining to Foreign Interests (DD Form 441s). In the case of a multiple facility organization, where more than one facility is covered by the DD Form 441 or DD Form 441—1, the contractor shall furnish a copy of the DD Form 441 with DD Form 441—1, when appropriate, to each facility covered under the Agreement and to the cognizant security office of each covered facility. Before a contractor is eligible for custody of classified information, he shall, in addition to having a facility clearance, have storage capability as prescribed in paragraph 14 and be prepared to apply the other safeguards prescribed by this Manual. Classified information which is of a higher security classification than the contractor's facility clearance may not be disclosed to the contractor.

b. Licensing, Patent and Trade Secret Agreements. Licensing, patent and trade secret agreements with a foreign entity may render a contractor ineligible for a facility security clearance unless appropriate procedures are established in the facility's SPP to insure that such agreements will not jeopardize the security of classified information which is entrusted to the contractor. In this connection, attention is directed to the State Department's ITAR, in particular Parts 124 and 125 thereof. This Regulation provides, *inter alia*, that before the execution of any license agreement envisaging the transmittal abroad of classified U.S. military information, it must first be submitted to the Department of State for review and approval, and that prior to any approval of such agreement, the release of the classified information involved must be approved by the cognizant U.S. military department and the DoD under established procedures.

c. Foreign Ownership, Control or Influence (FOCI). Facilities which are determined to be under FOCI are not eligible for a facility security clearance. Agreements with a foreign interest may make a contractor ineli-

gible for a facility security clearance. Execution of a DD Form 441s in accordance with instructions set forth in paragraph M, Appendix I, is required in connection with a determination of the degree, if any, of FOCI. The contractor must execute a new DD Form 441s when there is any change in the information previously submitted on the DD Form 441s. Any investor who has acquired a direct or indirect beneficial ownership interest of five percent or more of any class of stock of a registered company or any investor who plans to make a tender offer to purchase securities which is reasonably expected to result in such an ownership interest is required to file a Schedule 13 D report with the Securities and Exchange Commission, the company whose securities are involved and any national exchange on which the securities may be traded. If the acquisition will result in the submission of a revised DD Form 441s, and the contractor has received a Schedule 13 D from the investor, a copy of the Schedule 13 D will be forwarded with the DD Form 441s or, if appropriate, with the report (notification letter) required by paragraph 6a(4)(f). A new DD Form 441s shall also be executed by the contractor whenever advised that the form is required for an official purpose. It is the contractor's responsibility to provide complete information to assure that the degree of FOCI to which the facility may be subjected is fully explained so that the Government can ascertain that the security of the classified information in the possession of the contractor will not be jeopardized. A copy of the DD Form 441s and instructions for its completion are contained in paragraph M, Appendix I.

22. Personnel Clearances Required in Connection with Facility Clearances

The following individuals shall be cleared by the cognizant security office in connection with the facility security clearance, unless notified by the cognizant security office that such clearances are not required.

a. Corporations, Associations and Non-Profit Organizations.

- (1) Chairman of the board and all principal officers, such as president, senior vice president, secretary, treasurer, and those occupying similar positions see paragraph 3au). Other officers, who shall not require access to classified information in the conduct of the organization's business and who do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts, are not required to be cleared, provided the organization complies with the provisions of paragraph e, below.
- (2) All directors, unless one of the following options is elected:
 - (a) Directors, who shall not require access to classified information in the conduct of the organization's business and who do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts, are not required to be cleared, provided at least a legal quorum of the board of directors or similar executive body shall be cleared and, if the corporation or association conducts meetings with a pro tem chairman or by a rotating chairmanship, all board members who are eligible for or who could sit as board chairman shall be cleared; and, with respect to all uncleared directors, the organization complies with the provisions of paragraph e, below; or
 - (b) If the board has seen fit to delegate certain of its duties

and responsibilities to a legally constituted executive committee, all members of this committee shall be cleared. Other directors are not required to be cleared provided the committee has full executive authority to exercise management control and supervision for the corporation, including responsibility over all matters involving the security of classified information in the possession of the organization, and provided further, with respect to all uncleared directors, the organization complies with the provisions of paragraph e, below. Directors who are not members of this executive committee may be cleared but only at the same level as the facility clearance and when this is done, paragraph e, below, would not be applicable. Two copies of the board of directors' resolution delegating this authority to the committee shall be furnished to the cognizant security office.

- (3) Executive Personnel (see paragraph 3aa). The management official in charge at the facility and the security supervisor shall always be cleared in connection with the facility security clearance.
- (4) The corporation shall furnish a list of all officers, directors and executive personnel to the cognizant security office. The list shall designate by name those individuals granted a Letter of Consent, those who are being processed for a security clearance, and those who have been excluded from the requirement for a security clearance pursuant to the provisions of paragraph e, below. Such lists shall be signed by an offi-

cer, director or executive personnel of the corporation.

b. For Sole Proprietorships.

- (1) The Owner.
- (2) All Officers, if applicable.
- (3) Executive Personnel (see paragraph 3aa). The management official in charge at the facility and the facility security supervisor shall always be cleared in connection with the facility security clearance.
- (4) The sole proprietorship shall furnish a list of the owners, officers and executive personnel to the cognizant security office. The list shall designate by name those individuals granted a Letter of Consent, those who are being processed for a security clearance, and those who have been excluded from the requirement for a security clearance pursuant to the provisions of paragraph e, below. A current list shall be furnished once each year. Such lists shall be signed by the owner or by an officer or executive personnel of the sole proprietorship.

c. For Partnerships.

- (1) All General Partners. If the partnership has seen fit to delegate certain of its duties and responsibilities to a legally constituted executive committee, the members of this committee shall be cleared. Other partners, who shall not require access to classified information, are not required to be cleared provided the committee has full
 → executive authority to exercise management control and supervision for the organization, including
 → responsibility over all matters involving the security of classified information in the possession of the organization and, provided further,

paragraph e, below is complied with in respect to all uncleared general partners. (General partners who are not members of this executive committee may be cleared but only at the same level as the facility clearance and when this is done paragraph e, below would not be applicable.) Two copies of the partnership's resolution delegating this authority to the committee shall be furnished to the cognizant security office.

- (2) All Other Partners. Partners, other than general partners, who shall not require access to classified information in the conduct of the organization's business and who do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts, are not required to be cleared provided the organization, by official action of the general partners complies with the provisions of paragraph e, below. All partners who are cleared shall be cleared to the same level as the facility clearance.
- (3) Executive Personnel (see paragraph 3aa). The management official in charge of the facility and the facility security supervisor shall always be cleared in connection with the facility security clearance.
- (4) The partnership shall furnish a list of all partners and executive personnel to the cognizant security office. The list shall designate by name those individuals granted a Letter of Consent, those who are being processed for a security clearance and those who have been excluded from the requirement for a security clearance pursuant to the provisions of paragraph e, below. A current list shall be furnished once

each year. Such lists shall be signed by a partner or executive personnel of the partnership.

d. Colleges and Universities.

(1) The Chief Executive Officer.

(2) Those other officers or officials who are specifically and properly designated by action of the board of regents, board of trustees, board of directors or similar type executive body in accordance with the institution's requirement, as the managerial group having the authority and responsibility for the negotiation, execution, and administration of User Agency contracts. The institution shall furnish the cognizant security office a copy of such designation of authority, from which the particular officers who are to be processed in conjunction with a facility security clearance can be determined, and thereafter a current list shall be provided once each year. If this requirement is not met, all officers shall be processed for personnel security clearances.

(3) All regents, trustees, or directors, unless one of the following options is elected:

(a) Regents, trustees, or directors, who shall not require access to classified information in the conduct of the organization's business and who do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts, are not required to be cleared, provided at least a legal quorum of the board of regents, board of trustees, board of directors or similar executive body shall be cleared and, if the college or

university conducts meetings with a pro tem chairman or by a rotating chairmanship, all board members who are eligible for or could sit as board chairman shall be cleared; and, with respect to all uncleared regents, trustees or directors, the organization complies with the provisions of paragraph *e*, below; or

(b) If the board has seen fit to delegate certain of its duties and responsibilities to a legally constituted executive committee, all members of this committee shall be cleared. Other regents, trustees or directors are not required to be cleared, provided the committee has full executive authority to exercise management control and supervision for the organization, including responsibility over all matters involving the security of classified information in the possession of the organization, and provided further, with respect to all uncleared regents, trustees or directors, the organization complies with the provisions of paragraph *e*, below. Regents, trustees, or directors, who are not members of this executive committee, may be cleared but only at the same level as the facility clearance and when this is done paragraph *e*, below would not be applicable. Two copies of the board of directors' or similar executive body's resolution, delegating this authority to the committee shall be furnished to the cognizant security office; or

(c) If the board has seen fit to delegate all of its duties and responsibilities pertaining to

the protection of classified information to a managerial group comprised of officers or officials of the college or university, and if because of this delegation the board will not be in a position to affect adversely the performance of classified contracts, the board may exclude itself from the requirement for its members to be processed for a personnel security clearance by complying with the provisions of paragraph *e*, below. Election of this alternative will not preclude a regent, trustee or director from being processed for a personnel security clearance, if such clearance is necessary in connection with the individual's duties other than in the capacity of a regent, trustee or director. However, in such cases the clearance shall be at the same clearance level as the facility clearance. Two copies of the resolution by the board of regents, trustees, directors or similar executive body excluding the board members from access to classified information and delegating such authority to the managerial group shall be furnished to the cognizant security office.

- (4) Executive Personnel. The management official in charge of the facility and the facility security supervisor shall always be cleared in connection with the facility security clearance.
- (5) The college or university shall furnish a list of all personnel required to be cleared in connection with the facility security clearance pursuant to paragraphs (1) thru (4) above, or excluded to the cognizant

security office. The list shall designate by name those individuals granted a Letter of Consent, those who are being processed for a security clearance and those who have been excluded from the requirements for a security clearance pursuant to the provisions of paragraph *e*, below. A current list shall be furnished once each year. Such lists shall be signed by a regent, trustee, director or executive personnel of the college or university.

e. Exclusion Procedures. Those officers, directors, partners, regents and trustees who, pursuant to the provisions set forth above, can be excluded from the requirement for a personnel security clearance need not be processed for a clearance provided the organization, by formal action of the board of directors, all general partners or similar type executive body, affirms that—

- (1) Such officers, directors, partners, regents or trustees (designated by name) shall not require, shall not have, and can be effectively excluded from, access to all classified information in the possession of the organization and do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts or programs for the User Agencies. This action shall be made a matter of record in the organization's minutes of the partnership, board of directors, regents, trustees, or similar type executive body. Two copies of such minutes, dated and identified by the name and address of the facility, shall be furnished to the cognizant security office.
- (2) In case the organization does not comply with this requirement, all officers, directors, partners, regents, or trustees shall be processed for

clearances. Personnel who have been excluded from the requirement for a personnel security clearance in accordance with this paragraph shall not be processed for a clearance at a level lower than the facility clearance.

f. Representative of a Foreign Interest. When a representative of a foreign interest (see paragraph 3bb) is required to be cleared in connection with a facility clearance, and the representative of a foreign interest has not been excluded in accordance with paragraph e, above, the following procedures shall apply.

- (1) When the statement required by paragraph 20k has been executed, official notice of its execution shall be made a matter of record in the organization's minutes by the board of directors or similar type executive body. Two copies of the minutes shall be furnished the cognizant security office.
- (2) Failure to obtain a personnel security clearance for, or to exclude a representative of a foreign interest, shall make the facility ineligible for clearance, and any existing clearance shall be administratively terminated by the cognizant security office. Such action is not appealable.
- (3) In those cases where an individual who is cleared in connection with the facility security clearance becomes a representative of a foreign interest, the contractor shall submit the report required by paragraph 6a(4), in addition to the actions prescribed in this paragraph.

23. Security Clearance of Negotiators

Negotiators (see paragraph 3at) designated by the contractor as being required to participate in the preparation of a bid or

quotation may be processed for personnel security clearances concurrent with, but not as a part of, the facility security clearance. A facility security clearance is not dependent upon the clearance of negotiators and changes in negotiators shall not affect the status of a facility security clearance. Subsequent to the issuance of a facility security clearance, negotiators are processed for personnel security clearances in the normal manner prescribed by paragraph 26.

24. Security Clearance of Additional Personnel

Except in the case of personnel who are required to be cleared in connection with a facility security clearance as prescribed by paragraph 22, and negotiators as prescribed in paragraph 23, the contractor shall not initiate personnel security clearance actions on employees until a facility security clearance has been granted to the contractor. Contractor employees, other than those cleared in accordance with the provisions of paragraphs 22, 23, 27, 31, and 41e, whose access to classified information is essential in the performance of a classified contract, shall be cleared as specified below:

a. Clearance by the DoD. The DoD shall grant personnel security clearances for—

- (1) U.S. citizen employees of the contractor who—
 - (a) Require access to information classified TOP SECRET¹ or SECRET, or to any COMSEC information, regardless of classification, SENSITIVE COMPARTMENTED INFORMATION or RESTRICTED DATA; or

¹ When a TOP SECRET clearance is requested, DISCO will automatically issue a Letter of Consent for SECRET when the investigation necessary for clearance at the SECRET level has been completed with satisfactory results. That Letter of Consent will subsequently be superseded by a Letter of Consent for TOP SECRET when the required additional investigation is completed.

- (b) Are employed by a college or university; or
 - (c) Require access to NATO information classified CONFIDENTIAL or higher as described in Section XI; or
 - (d) Require access to ACDA classified information; or
 - (e) Make determinations to grant access authorizations in accordance with paragraph b, below; or
 - (f) Are representatives of a foreign interest; or
 - (g) Require security clearance as a condition of the Nuclear Weapon PRP for duties in Critical and Controlled positions under the nuclear weapon security program (see paragraph 3at.1).
- (2) Immigrant alien employees of the contractor who require access to SECRET or CONFIDENTIAL information. Immigrant aliens are not eligible for access to SENSITIVE COMPARTMENTED INFORMATION, COMSEC, NATO information (see paragraphs 6b(6), 20c, 20m, 75 76, 85d, and 86), or for performance of duties in Critical or Controlled positions under the nuclear weapon security program (see paragraph 3at.1). Moreover, immigrant aliens are not eligible to be processed for DoD clearances at the TOP SECRET level.
- (3) Employees of the contractor whose application for clearance is referred to DISCO according to paragraph b(4), below.
- b. Clearance by the Contractor.* Employees of the contractor not covered by paragraph a, above who are U.S. citizens and who require access to information classified no higher than CONFIDENTIAL, shall be cleared by the contractor as prescribed below. Such clearances shall remain valid, unless otherwise revoked, within any facility of the same organization so long as the individual continues in the contractor's employment. However, if the employee no longer has or requires access to classified information and no future requirement for such access is anticipated in the foreseeable future, clearance can be administratively terminated by complying with paragraph 29. The contractor is not authorized to grant an interim CONFIDENTIAL clearance. Contractor granted CONFIDENTIAL clearances are not valid for access to RESTRICTED DATA, COMSEC information, SENSITIVE COMPARTMENTED INFORMATION, ACDA classified information; or NATO information; except for NATO RESTRICTED information.
- (1) The clearance shall be based upon the contractor's determination that—
- (a) The employment records of the employee are in order; and
 - (b) The Application and Authorization for Access to Confidential Information (Industrial) (DD Form 48-2) executed by the employee indicates that (i) the employee is a U.S. citizen and not a representative of a foreign interest; (ii) the information furnished in item 8, if any, does not reflect that a personnel security clearance has been suspended, denied, or revoked in his case.
 - (c) There is no information known to the contractor which would

indicate that the employee's access to classified information is not clearly consistent with the national interest.

- (2) When the response to item 7 indicates that the applicant has applied for or received a previous security clearance, and there is no indication in the applicant's response to item 8 that a prior clearance has ever been suspended, denied, or revoked, the contractor may grant the CONFIDENTIAL clearance if otherwise appropriate. However, a copy of the DD Form 48-2 shall be sent to DISCO for a check of the PSCF.
- (3) Before an individual signs the DD Form 48-2 he should read the certification statement. After he signs in the presence of the witness, the witness shall affix his signature and address.
- (4) When the determination required in paragraph (1) above cannot be made, or if the employee will not sign the DD Form 48-2, the contractor shall forward the application for CONFIDENTIAL clearance, together with the forms prescribed in paragraph 26c, to DISCO for appropriate action.
- (5) An affirmative answer to question 11 or an answer to question 12 indicating that the applicant has relatives living in a Communist country will not, in itself, preclude a determination by the contractor that an employee is eligible for a CONFIDENTIAL clearance, where all other available information indicates that access is clearly consistent with the national interest. In such cases, where the contractor grants a CONFIDENTIAL clear-

ance, he shall forward promptly to DISCO one copy of DD Form 48-2 together with the forms prescribed in paragraph 26c, for further evaluation and determination of continued eligibility for access to CONFIDENTIAL information.

- c. The contractor is not authorized to revoke a clearance that he has granted.

25. Preemployment Clearance Application—Prohibited

The contractor shall not initiate any pre-employment clearance action. An applicant for employment in a position which requires access to classified information may be informed that a security clearance will be required and that a security clearance can only be granted to: (i) U.S. citizens; (ii) immigrant aliens who reside and intend to reside permanently in the U.S. (including Puerto Rico, Guam and the Virgin Islands); or (iii) citizens of Canada or the U.K. A Personnel Security Questionnaire (Industrial) (DD Form 48), DD Form 48-2, Personnel Security Questionnaire (Updating) (DD Form 48-3), Personnel Security Questionnaire (Industrial) (Multiple Purpose) (DD Form 49), or Worksheet for the Preparation of Personnel Security Questionnaires (DLA Form 707) shall not be offered to or be required to be completed by an individual until he is employed by the contractor in a position requiring access to classified information and placed on the payroll. However, in exceptional cases where a written contract for future employment in a position which requires access to classified information has been executed by both parties with a fixed date for entry on the payroll, the personnel security clearance application forms may be furnished to and executed by the employee prior to the date of entry on duty provided the actual date of entry on duty under such written contract is not contingent upon issuance of a personnel security clearance.

26. Application for Personnel Security Clearance

a. General

- (1) Contractors shall make application for DoD security clearances in accordance with the provisions of this Section. For personnel clearances required in connection with a facility security clearance under paragraph 22, applications shall be submitted to the cognizant security office. Application for all other personnel clearances shall be submitted to DISCO, P.O. Box 2499, Columbus, Ohio 43216. In addition to the forms required in connection with the application for a personnel security clearance, the forms required by paragraph *c*, below shall be accomplished and submitted when requested to satisfy an official requirement by DISCO or the cognizant security office. Failure by the employee concerned to furnish the forms when requested or when required by this Manual, in connection with a clearance application, shall preclude the granting of any new security clearance with respect to the employee concerned, and shall constitute sufficient reason for considering revocation with respect to any outstanding security clearance covering the employee concerned. Whenever a contractor employee has submitted forms prescribed by this paragraph to DISCO but subsequently objects, for any reason, to be processed for a clearance or to have an existing clearance continued, the contractor shall submit a report to DISCO. Verification of such objections shall be made by the Government. After verification, any pending clearance shall be terminated and any security clearance then held by the employee shall be administratively

terminated by the Government without prejudice to the employee.

- (2) The contractor shall establish adequate procedures to assure that Part II of the DD Form 48, or the DD Form 49; or Part I of the DD Form 48-3, as appropriate, is completed prior to completion of any other part of the form by the employee. Additionally, the contractor will insure that Part III, DD Forms 48, 49, or 48-3, as appropriate, is completed by the employee in private. Moreover, the employee shall be advised of the instructions which preface Part III, relating to the completion of Part III in private, and the provision for adding any additional information which he may consider to have a bearing on his security clearance.
- (3) Moreover, the employee shall be advised that prior to affixing his signature to the form, the form shall be folded so that the witness to his signature will not see any portion of Part III of the completed PSQ. After the employee signs the original in the presence of the witness, the witness shall affix his signature and address.
- (4) The employee shall be further advised that, upon completion of the above, the form shall be inserted by him in the pre-addressed envelope (DLA Form 703) provided, together with the previously completed Fingerprint Card (FD Form 258). For personnel security clearances required in connection with a facility security clearance, the application shall be submitted to the cognizant security office by use of the envelope (DLA Form 704) provided which requires affixing the address of the appropriate cognizant security office together with

DoD 5220.22-M

the previously completed FD Form 258. (The Fingerprint Card is not required when a DD Form 48-2 or DD Form 48-3 is submitted. It is required in connection with all other submissions.) The employee shall be advised that: (i) the envelope shall be sealed by him; (ii) his signature shall be affixed across the envelope flap on the line provided; (iii) the date of the signature will be inserted on the line provided; and (iv) the envelope shall be immediately returned to the employer for mailing.

- (5) The employer shall assure that the Fingerprint Card, if required, is completed prior to completion of the DD Form 48 or DD Form 49 so that it will be available for the employee to insert in the pre-addressed envelope upon completion of the DD Form 48 or DD Form 49. In addition, the contractor shall establish procedures to assure that an employee of the contractor will witness the taking of the employee's fingerprints on the card, to insure that the persons fingerprinted is, in fact, the same as the employee being processed for the clearance. The employer shall witness the placing of the Fingerprint Card in the envelope and the sealing of the envelope, to assure substitutions do not occur.
- (6) When the sealed envelope containing the completed personnel security forms is received from the employee by the contractor, it shall be forwarded unopened to DISCO, or to the cognizant security office, as provided in paragraph (1).
- (7) All forms required by this Section in connection with personnel security clearances shall be obtained from DISCO. Instructions for com-

pletion of such forms are contained in pamphlets, which are also obtained from DISCO. These pamphlets are entitled: (i) Instructions for Completion of DD Form 48 or DD Form 49; (ii) Instructions for Completion of DD Form 48-3; and (iii) Instructions for Completion of DD Form 48-2.

b. Immigrant Aliens. Prior to submitting an application for a personnel security clearance for an immigrant alien, the contractor shall require the alien to produce for the contractor's review, the Alien Registration Receipt Card (Form No. I-151) which has been issued to the individual. This card is issued only to aliens who have been lawfully admitted to the U.S. under an immigration visa for permanent residence.

c. New Clearances. Application for an initial clearance, for upgrading an existing clearance, or for requesting a clearance in situations where other provisions of this Manual are not applicable, shall be made by the contractor by submission of the following forms:

- (1) A DD Form 48² completed and executed by U.S. citizens who are to be processed for a DoD issued CONFIDENTIAL or SECRET clearance unless paragraph (2) below applies.
- (2) A DD Form 49³ completed and executed in the following cases:
 - (a) Immigrant aliens who are to be processed for SECRET or CONFIDENTIAL clearance.
 - (b) U.S. citizens who are to be

² The DD Form 48 packet is composed of the PSQ and one copy of the NAC Request (DD Form 1584).

³ The DD Form 49 packet is similar to the DD Form 48 packet but contains five copies of the PSQ and additional questions regarding citizenship status.

DoD 5220.22-M

processed for TOP SECRET clearance.

- (c) U.S. citizens who are to be processed for any level of clearance when the applicant lists relatives or relatives of his spouse who are residing in Communist countries (Communist countries are listed in footnote 10 to paragraph 5u).
 - (d) U.S. citizens who are to be processed for any level of clearance when the applicant advises he is a representative of a foreign interest.
- (3) A properly completed and executed FD Form 258 with each request submitted pursuant to paragraph (1) or (2). Care shall be exercised to insure that fingerprints are authentic, legible and complete, as those which do not meet prescribed standards shall be returned for re-execution which will result in clearance delays. The employee being processed for access shall insert all the forms in the pre-addressed envelope (DLA Form 703) provided, and then seal. The employee shall then place his signature and the date across the envelope flap on the line provided. The employee shall deliver the sealed, signed and dated envelope immediately to the designated company representative, who will insure mailing.

d. Interim Clearance. Except as authorized below, requests for interim personnel security clearances must be approved by the contracting officer. Contracting officer approval will be given only in an emergency situation in order to avoid crucial delays in precontract negotiation, or in the award or performance on a contract. The contractor shall (i) obtain such approval and submit

it with the application for interim clearance, or (ii) forward the application for interim clearance through the contracting officer. An application for an interim SECRET or CONFIDENTIAL clearance shall not be made when a request for a SECRET or CONFIDENTIAL clearance is already in process based on a previously submitted clearance application. The application for interim clearance shall consist of the forms prescribed by paragraph c, above. The words "Interim TOP SECRET," "Interim SECRET," or "Interim CONFIDENTIAL," as appropriate, shall be placed in bold letters in the lower right-hand corner of the "Job Title and Description of Duties" block of the DD Form 48 or 49. The approval letter from the contracting officer shall be attached behind the FD Form 258. As an exception to the foregoing procedures, and paragraph i., below, when an emergency situation exists which would render the facility incapable of adequately safeguarding classified material in its possession and no contracting officer is available to approve the interim clearance request within the time required to negate the threat, the cognizant security office is authorized to approve interim personnel security clearance requests being forwarded to DISCO. Interim SECRET clearances for immigrant aliens are not authorized. Access limitations applicable in the case of interim clearances are set forth in paragraph 20c.

e. Clearance Transfers. Application for a security clearance may be made by the contractor for employees for whom a Letter of Consent was previously issued while the individual was employed by another contractor provided there has not been a lapse of more than 12 months since termination of the employment for which the Letter of Consent was issued. Application is made by submitting one copy of an executed DD Form 48-3.

f. Clearance Transfers - Multiple Facility Organizations. When an employee for whom a Letter of Consent has been issued is transferred from one facility to another in a multiple facility organization with the same

DoD 5220.22-M

or higher level of facility security clearance, the contractor shall—

- (1) Forward to the gaining facility either a copy of the Letter of Consent for the employee being transferred, which shall be certified by the contractor of his authorized representative as a true copy; or the original Letter of Consent, if it lists only the employee being transferred.
- (2) Promptly submit two copies of DLA Form 562-R to DISCO as notification of the transfer.

However, when an employee is transferred to an uncleared facility or a facility with a lower level facility security clearance than the employee's clearance, and if the employee will continue to require access at the level of his clearance at another cleared facility or a Government installation, or if the contractor desires to retain the Letter of Consent at the higher level so it will be available in the event the individual is transferred back to a facility at which the clearance will be needed, the Letter of Consent shall be forwarded to the home office facility or the appropriate principal management facility of the multiple facility organization rather than to the gaining facility. If an employee is transferred to a facility with a lower level facility clearance than his personnel clearance and the contractor desires to retain the Letter of Consent only at the lower level, the contractor shall amend the Letter of Consent to reflect the lower level of the access authorization and include a statement to this effect in the "Remarks" block of the DLA Form 562-R which is submitted to DISCO. Clearance transfer action under this paragraph may be initiated after determination to reassign has been made, but prior to the actual transfer.

g. Concurrent Clearances

- (1) When a contractor hires an individual or engages a consultant on a

temporary or part-time basis, who is also employed by or acting as a consultant to another contractor, and who has a current Letter of Consent, an additional Letter of Consent shall be requested if the individual requires access to classified information. Application for a Letter of Consent will be made by the submission of one copy of an executed DD Form 48-3. The "Concurrent Clearance" block shall be marked on the DD Form 48-3.

- (2) An exception to the requirement for submission of a DD Form 48-3 to obtain a concurrent clearance can be made when an OODEP of a parent company becomes concurrently an OODEP of a subsidiary, or when an OODEP of a subsidiary becomes concurrently an OODEP of the parent company, provided the new clearance being requested is not at a higher level than the existing clearance. In these cases the contractor (parent or subsidiary) to whom the existing clearance has been issued, will submit a letter to the cognizant security office of the facility (subsidiary or parent) to which the new clearance is to be issued setting forth full name, date and place of birth, Social Security number, date and level of clearance of the OODEP, and request a concurrent clearance at the parent or subsidiary, as the case may be. After issuance of the concurrent clearance, the facility (parent or subsidiary) to which the new clearance has been issued will furnish a copy to the facility to which the initial clearance was issued. That facility in turn will furnish to the other facility, a reproduction of Part I of the DLA Form 482. If the OODEP'S employment is terminated at either facility, the cognizant security of-

office of that facility will be advised in accordance with established procedures. In addition, Part II of the DLA Form 482 will be completed and maintained in the records of that facility. If employment with the parent and subsidiary is terminated, their respective cognizant security offices will be notified in accordance with established procedures. Only one debriefing statement (Part II of DLA Form 482) need be completed, but a reproduction will be furnished the other facility.

- (3) Any action by the Government to suspend or revoke a clearance will be equally applicable to all concurrent clearances issued for the consultant or OODEP. Concurrent notices of such action will be provided each employer by the Government.

h. Reemployment of Cleared Personnel. When, within a period of 12 months, a contractor reemploys an individual for whom he had previously been issued a Letter of Consent, the contractor may reactivate the Letter of Consent by submitting a notice of reemployment on DLA Form 562-R to DISCO. Two copies of the form shall be submitted. Contractor-granted CONFIDENTIAL clearances of individuals who are reemployed within a period of 12 months may be reinstated by the contractor without notification to DISCO. Where the previously issued Letter of Consent was at the TOP SECRET level, and there is no valid requirement to reinstate the clearance at that level, the contractor may request a Letter of Consent at the SECRET level for the individual within a 12-month period by submitting two copies of DLA Form 562-R to DISCO, annotated in the "Remarks" section to indicate the lower level of clearance to be reinstated.

i. Formerly Cleared Personnel. In cases involving U.S. citizens where a final SECRET or final TOP SECRET clearance cannot

be transferred or cannot be reactivated because there has been a lapse of more than 12 months since termination of the employment for which the Letter of Consent was issued, the contractor may request an interim SECRET clearance without obtaining approval from the contracting officer, provided application is made within 25 months from the date of termination of the employment for which the Letter of Consent was issued. The application will be made by submitting the forms specified in paragraph *c*, above, to DISCO. Applications submitted pursuant to this paragraph shall be annotated in the "Job Title and Description of Duties" block of the DD Form 48 to indicate that interim clearance pursuant to paragraph 26*i* is requested. Where the previous clearance was issued at the CONFIDENTIAL level by the DoD, the contractor may request an interim CONFIDENTIAL clearance under the provisions of this paragraph.

j. Change of Name. The contractor shall submit one copy of DLA Form 562-R to DISCO whenever a change occurs in the legal name of an employee for whom the DoD has issued a Letter of Consent. Upon receipt of this report a new Letter of Consent will be issued.

k. Issuance of Letter of Consent.

- (1) Except as authorized below, Letters of Consent are issued to the facility at which the individual is principally employed and the name and address of this facility shall be entered in the "Name and Address of Employer" block of the DD Form 48 or 49. The exceptions applicable only in the case of multiple facility organizations are:

- (a) The employee (*i*) who, in connection with the performance of his duties at another cleared facility or Government installation, requires access to a higher category of classified information than the facility

DoD 5220.22-M

clearance of the facility at which he is employed or physically located, or (ii) who is employed or physically located at an uncleared facility. In such cases the Letter of Consent is issued to the home office or the appropriate principal management facility of the multiple facility organization and it may not be for a higher category of access than the facility clearance of the home office or the principal management facility.

- (b) When the contractor elects to have Letters of Consent issued to the home office or a principal management facility rather than to the facility at which the individuals are employed or physically located. Prior to requesting DISCO to send Letters of Consent to a home office or principal management facility, the contractor shall develop a proposed SPP or a proposed procedure for inclusion in the existing SPP and forward it to the cognizant security office of the home office or the principal management facility for review. The SPP shall identify (i) each facility of the multiple facility organization, or (ii) each facility of the multiple facility organization which is located within the geographical or functional area for which the principal management facility is administratively responsible. Upon receipt of notice from the cognizant security office that the SPP is adequate, the contractor may request DISCO to issue Letters of Consent to the home office or principal management facility.

- (c) When the individual is required to be cleared in connection with the home office facility clearance and his principal place of work is at another facility of the multiple facility organization. In this case, Letters of Consent are issued to both the home office facility and the facility where the individual is principally employed or physically located, or to the appropriate principal management facility. An additional Letter of Consent may be issued upon submission of a DLA Form 562-R which shall indicate in the "Remarks" section the reasons therefor.

- (2) When the Letter of Consent is issued to the home office or principal management facility rather than the facility at which the individual is principally employed or physically located, the contractor is required to:

- (a) Maintain a clearance record at the facility where the individual is employed or physically located. In addition, the home office or principal management facility shall maintain records which reflect:

1. The facility at which the individual is employed or physically located;
2. The date(s) of initial and recurring security briefings, and the name(s) of the briefer(s); and
3. The date(s) and name(s) of the officials conducting visits to the uncleared facilities pursuant to paragraph 73.

- (b) Report transfers within the multiple facility organization in accordance with paragraph *f*, above; and,
 - (c) Process visits to other facilities of the multiple facility organization in accordance with paragraphs 41*a* and 73.
- (3) On the application for clearance submitted pursuant to paragraphs *k*(1) (a) and (b) above, the DD Forms 48, 49, or 48-3, or DLA Form 562-R shall clearly indicate the name and address of the facility at which the individual is employed or physically located in the "Name and Address of Employer" block of the form. In addition, the name and address of the facility to which the Letter of Consent is to be mailed shall be placed in the "Job Title" block of the DD Form 48, 49, or 48-3, or the DLA Form 562-R. The facility name and address shall be preceded by the words "MAIL TO" in bold letters.

l. ERDA Clearances. A contractor who is engaged in classified work with the ERDA may request a DoD industrial personnel security clearance for an employee who holds a "Q" or "L" clearance in connection with the contractor's work for the ERDA. In such cases, the "Q" clearance shall be considered as an authoritative basis for a DoD clearance at the SECRET level provided the investigative basis of the "Q" clearance meets DoD investigative requirements. The "L" clearance shall be considered as an authoritative basis for a DoD clearance at the CONFIDENTIAL level, provided the investigative basis of the "L" clearance meets DoD investigative requirements. Application for an industrial personnel security clearance based on a "Q" or "L" clearance may be made by the submission of one copy of DD Form 48-3 to DISCO. The "Job Title and Description of Duties" block in Part I of the DD Form 48-3 will be annotated "ERDA

"Q" (or "L") Conversion Requested." The DISCO will obtain verification of the current "Q" or "L" clearance and the investigative basis thereof from the ERDA. Following this verification DISCO will issue a Letter of Consent to the contractor.

27. Clearance of Present and Former Civilian and Military Personnel of the DoD and Certain Other Government Agencies

a. Personnel security clearances issued by a User Agency to civilian or military personnel who are U.S. citizens may be converted to industrial personnel security clearances as follows:

- (1) Top-level civilian or military personnel—18 months from the time of separation from active Federal service.
- (2) Retired civilian and military personnel of any grade with 19 years or more of Federal service—18 months from the date of retirement from active Federal service.
- (3) For other civilian or military personnel separated or retired from active Federal service—12 months from the time of separation or retirement from active Federal service.
- (4) Reserve military personnel who are not on extended active duty but who actively participate in a Reserve program requiring that they hold a valid security clearance, may have such clearance converted to an industrial security clearance. Clearances granted to such personnel who have transferred to the standby or retired Reserve also may be converted to industrial security clearances within 12 months of a person's being placed in the standby or retired Reserve. Clearances granted to members of the Na-

tional Guard are not convertible to industrial security clearances.

b. Personnel security clearances issued by other Departments or Agencies of the Executive Branch of Government to personnel who are U.S. citizens, may be converted to industrial personnel security clearances when:

- (1) A determination can be made, based upon a review of the prior investigation, that the investigation meets standards prescribed by the DoD for such clearances;
- (2) The service of the employee, in a cleared status, has been continuous since the investigation with no break in service longer than 12 months; and
- (3) An inquiry to the employee's previous employer or employers discloses no reason for expanding or updating the investigation.

c. Top-level civilian personnel are defined as Presidential appointees, Civil Service appointees of the supergrades (GS-16 and above) and members of Industry Advisory Committees who have been duly appointed by Secretariat levels of the User Agencies. Top-level military personnel are those of the general and flag officer grades.

d. Contractors employing personnel eligible for conversion of clearance under the provisions of this paragraph may request clearance to the level of access required in the assignment of their duties by submitting the following information:

- (1) One signed copy of DD Form 48-3.
- (2) For former civilian personnel—an exact reproduction of the Notification of Personnel Action (Standard Form 50) which terminated his employment with the Government.
- (3) For former military personnel—an exact reproduction of the Armed Forces of the United States Report of Transfer or Discharge (DD Form 214).

(4) For civilian or military personnel presently employed by or on active duty with a User Agency, the forms prescribed by paragraph (2) or (3) above are not required. However, in the case of military personnel the individual's service number shall be placed in Item 18 of the DD Form 48-3.

(5) For Reservists participating in a Reserve Program and for those who have transferred to the standby or retired Reserve within the past 12 months, the forms prescribed by paragraph (2) or (3) above are not required. However, the individual's service number, the identity and exact address of the unit to which assigned and the date such participation commenced shall be placed in item 18 of the DD Form 48-3. In addition, for those individuals who have transferred to the standby or retired Reserve, a copy of the orders effecting such a transfer shall be attached to the DD Form 48-3.

e. The complete set of forms required by paragraph 26c shall be accomplished when:

- (1) The clearance requirement is for a higher level than is reflected in the clearance records; or
- (2) There has been greater lapse of time than that set forth in paragraph a, above; or
- (3) Requested by DISCO. (The request will state that the forms are needed to satisfy an official requirement.)

28. Contractor's Clearance Record

The contractor shall maintain a current record at each facility of all employees and consultants located at the facility who have been cleared for access to classified informa-

tion. The record will indicate the level and date of clearance and whether cleared by a specific military department, DISCO or the contractor.

29. Administrative Termination of Personnel Security Clearances

a. The contractor, under the conditions stated below, may request the administrative termination of SECRET and Government granted security clearances which are no longer required. If a cleared employee no longer has or requires access to classified information and no requirement for such access is anticipated in the foreseeable future, administrative termination of a Government issued clearance is accomplished by submission of a properly completed Request for Administrative Termination of Personnel Security Clearance (DLA Form 683) to DISCO. Contractor granted CONFIDENTIAL clearances may be administratively terminated by the contractor in accordance with the procedures and criteria of this paragraph. The contractor shall process for administrative termination, or downgrading to a lower level (see paragraph 30) all TOP SECRET clearances which are no longer required. When an individual with a TOP SECRET clearance has not had access to TOP SECRET information in the previous 18 months, but the contractor anticipates a requirement for access to TOP SECRET information in the foreseeable future, justification for retention of a TOP SECRET personnel clearance shall be provided the cognizant security office. If a contractor fails to take action to terminate a TOP SECRET personnel security clearance under the conditions described above, and fails to submit justification for retention of the clearance, the cognizant security office shall submit a recommendation to the EDIS, HQ DLA, for processing pursuant to the provisions of paragraph f., below.

b. If the contractor determines that an

individual previously cleared in connection with the facility clearance no longer requires clearance and can be excluded from access in accordance with the procedures set forth in paragraph 22e, a recommendation for administrative termination of the clearance may be submitted to the cognizant security office by submission of a properly completed DLA Form 683 and two copies of the organization's minutes attesting that the exclusion action required by paragraph 22e(1) has been completed.

c. In connection with the preparation of the DLA Form 683 the contractor shall advise the employee as follows:

- (1) The personnel security clearance shall be administratively terminated since there is no current or foreseeable future requirement for access to classified information;
- (2) The proposed action in no way reflects adversely upon the employee's personnel security eligibility;
- (3) The employee may be processed for a new personnel security clearance with a minimum of delay when the occasion and need arise for the employee to require access to classified information; and
- (4) The employee's signature on the DLA Form 683 will certify that he understands and acknowledges this action.

d. At the time the employee signs DLA Form 683 he will also be debriefed in accordance with paragraph 5g and requested to sign Part II of DLA Form 482. On completion of DLA Form 683 by the employee the contractor will forward the form to DISCO. (In the case of an OODEP the DLA Form 683 shall be forwarded to the cognizant security office.) The completed DLA Form 482 will be retained by the contractor in accordance with paragraph 5g. In the case of the administrative termination of a contractor granted CONFIDENTIAL clearance,

CH 1

DoD 5220.22-M

DLA Form 683 will be retained by the contractor for 2 years along with DLA Form 482. The administrative termination of a contractor granted CONFIDENTIAL clearance is completed at the time the employee signs DLA Form 683. As provided for in paragraphs 29 and 30, if subsequent to such termination it becomes necessary to revalidate the clearance, Part I of the DLA Form 482 will be executed prior to the person having access to classified information.

e. If the employee will not sign the DLA Form 683, the contractor shall refer the matter to the cognizant security office for determination. Included with the letter of referral shall be the partially completed DLA Form 683. The contractor shall also furnish the home address of the employee. The cognizant security office will contact the employee and request him to show cause as to why the recommended action should not be completed. If the individual fails to respond within 30 days from receipt of such request to show cause, the Government will consider such failure as notice to the Government that the individual no longer objects to the administrative termination of the clearance.

f. In those rare and exceptional cases where DASD(SP), or higher authority, determines that a personnel security clearance was granted in error or is not required, he may, at his option, administratively terminate the clearance or clearance action in process without prejudice to the individual concerned or jeopardy to his employer's operations.

g. In the event a need arises for an employee to have access to classified information subsequent to the administrative termination of his clearance, and such need occurs within 24 months from date of notice from the Government that the previous clearance was administratively terminated, the previous clearance may be revalidated immediately provided (i) the individual has been continuously employed by the same contractor, and (ii) the contractor knows of no

questionable or adverse information concerning the employee. Revalidation will be effected by submission of two copies of DLA Form 562-R to DISCO or the cognizant security office, as appropriate. The DISCO will revalidate the clearance. The statement, "This is a request for revalidation of a clearance administratively terminated on (date)" shall be included in item 13, "Remarks."

h. In the event an employee for whom a Letter of Consent was administratively terminated is transferred from one facility to another in a multiple facility organization with the same or higher level of facility security clearance, and the gaining facility has a need for the employee to have access to classified information, and such need occurs within 24 months from date of notice from the Government that the previous clearance was terminated, the previous clearance may be revalidated provided (i) the individual has been continuously employed by the same contractor, and (ii) the contractor knows of no questionable or adverse information concerning the employee. Revalidation will be effected by submission of two copies of DLA Form 562-R to DISCO or the cognizant security office, as appropriate. The DISCO will revalidate the clearance. The block "multiple facility transfer" will be checked in item 1, and the statement, "This is a request for revalidation of a clearance administratively terminated on (date)" shall be included in item 13, "Remarks."

i. In the event an employee for whom a Letter of Consent was administratively terminated is employed by another contractor in a position requiring access to classified information, and such employment occurs within 12 months from date of notice from the Government that the previous clearance was terminated, the previous clearance may be revalidated by submission of one copy of an executed DD Form 48-3. The DISCO will reissue the clearance by forwarding a new Letter of Consent to the contractor.

j. If the previous clearance which was administratively terminated was a contractor-

granted CONFIDENTIAL clearance, and a new need arises for the individual to have access to CONFIDENTIAL information, the actions required by paragraph 24b, shall be accomplished as a new clearance action.

30. Administrative Downgrading of TOP SECRET Personnel Security Clearances

a. When an employee other than an OODEP, cleared at the TOP SECRET level, has not had access to TOP SECRET information during the preceding 18 months, and a requirement for such access is not anticipated, but access to a lower category of classified information is required, the personnel security clearance shall be downgraded without prejudice to a lower level by submission of a DLA Form 562-R, in duplicate, to DISCO. The properly completed form shall set forth in the "Remarks" block, item 13, a request to downgrade the TOP SECRET clearance without prejudice to the appropriate level. Upon receipt of a copy of the DLA Form 562-R from DISCO, annotated to reflect that the requested action has been completed, the contractor shall annotate the previously issued Letter of Consent to reflect the new level of access, and the date such action was taken by DISCO. The Letter of Consent retains the original date of issuance.

b. TOP SECRET personnel security clearances downgraded in accordance with the paragraph can be reinstated summarily upon request of the contractor, when a requirement for such access exists, provided (i) there has not been a lapse of more than 24 months from the date of the downgrading or termination action, (ii) the individual has been continuously employed by the same contractor/multiple facility organization, (iii) the contractor knows of no questionable or adverse information concerning the employee and (iv) that a valid need exists for the revalidation of the TOP SECRET clearance. Application is made by submission of DLA

Form 562-R, in duplicate, to DISCO setting forth in the "Remarks" block, item 13, a request to reinstate the previous TOP SECRET clearance. Upon receipt of a copy of the DLA Form 562-R from DISCO, annotated to reflect that the requested action has been completed, the contractor shall annotate the previously issued Letter of Consent to reflect the new level of access and the date such access was authorized by DISCO.

c. When there has been a lapse of more than 24 months from the date the TOP SECRET clearance was downgraded to a lower level clearance, DISCO will issue a new Letter of Consent provided (i) the individual has been continuously employed by the same contractor/multiple facility organization since the date of the downgrading action, (ii) the contractor knows of no questionable or adverse information, and (iii) that a valid need exists for the TOP SECRET clearance. Application for the new Letter of Consent shall be made by submitting one copy of DD Form 48-3 to DISCO.

31. Canadian and U.K. Reciprocal Clearances

a. Pursuant to the provisions of The United States-Canada Industrial Security Agreement, employees of the contractor who are citizens of Canada, except those individuals who have status as aliens admitted to the U.S. under an immigration visa for permanent residence, may be processed for a Canadian Reciprocal clearance authorizing access to classified information in connection with the performance of classified work at a facility located in the U.S. or Canada.

b. Under the provisions of the U.S.-U.K. Industrial Security Agreement, employees of the contractor who are citizens of the U.K., except those individuals who have status as aliens admitted to the U.S. under an immigration visa for permanent residence, may be processed for a U.K. Reciprocal clearance authorizing access to classified information in connection with the performance of clas-

CH 1

DoD 5220.22-M

sified work at a facility located in the U.S.

c. Application for Canadian or U.K. Reciprocal clearances for employees in the categories described in paragraphs *a*, and *b*, above shall be made by the contractor by submission of the DD Form 49 and three copies of executed FD Form 258. The following items on the DD Form 49 need not be completed and the notation "not applicable" may be used in lieu thereof: 13*d*(1); 13*d*(4) thru 13*d*(7); and 15*b*. Item 19 need only be answered with respect to non-U.S. or non-Canadian organizations where the application is for a Canadian Reciprocal clearance; and non-U.S. and non-U.K. organizations where the application is for a U.K. Reciprocal clearance. The words "RECIPROCAL CLEARANCE" shall be placed in bold, block letters in the lower right-hand corner of the "Job Title and Description of Duties" block of the DD Form 49.

d. Limitations on Access Under Reciprocal Clearances (Both Facility and Personnel Security Clearances).

(1) Canadian and U.K. Reciprocal clearances granted under the provisions of this paragraph are not valid for access to:

- (a) RESTRICTED DATA, as defined in the U.S. Atomic Energy Act of 1954, as amended;
- (b) FORMERLY RESTRICTED DATA removed from the RESTRICTED DATA category

pursuant to Section 142(*d*) of the U.S. Atomic Energy Act of 1954, as amended;

- (c) COMSEC information;
- (d) Any ACDA classified information;
- (e) Information for which foreign dissemination has been prohibited in whole or in part;
- (f) Any information for which a special access authorization is required; and
- (g) Any information which has not been specifically authorized for release to either Canada or the U.K. as the case may be.

(2) In addition, Canadian Reciprocal clearances are not valid for access to classified atomic energy data as defined in the Atomic Energy Control Act (Revised Statutes of Canada 1952) and the Atomic Energy Control Regulations, Order-in-Council PC, 1959-1643.

e. Individuals who have been granted Canadian or U.K. Reciprocal clearances, and who subsequently become immigrant aliens or U.S. citizens, need not be processed for regular clearance, pursuant to paragraph 26, unless a requirement arises for access to information set forth in paragraph *d*, above or for information of a higher classification category than covered by the Canadian or U.K. Reciprocal clearance.

SECTION IV

CONTROL OF AREAS

32. Purpose

Normally, the contractor shall protect classified material in the manner prescribed in paragraphs 14, 15, and 16. If, however, because of the nature, size or unique characteristics of the classified material, unauthorized personnel cannot be effectively denied access to such material by the safeguards set forth in the above paragraphs, the material shall be safeguarded by controlling the area in which it is located.¹ Controlled areas shall consist of Closed and Restricted Areas as defined in paragraphs 3*h* and 3*bc*, respectively.

33. General

a. A controlled area shall not be established for the sole purpose of storing classified documents (see paragraph 14*a*(3)(*f*) for guidance on use of "other vaults and strongrooms" for the storage of classified documents).

b. The frequency of the guard patrols (see paragraph 34*a*(3) below) shall be determined primarily by the construction features of the area. If the area is constructed as described in Appendix V, a patrol of the area once every two hours is sufficient. If the area is constructed using standards lesser than in Appendix V, then the frequency of patrol has to be increased.

¹ The entry into a controlled area, per se, will not constitute access to classified information if the security measures which are in force prevent the gaining of knowledge of the classified information. Therefore, the entry into a controlled area under conditions that prevent the gaining of knowledge of classified information will not necessitate a personnel security clearance.

c. Area designations shall be promptly removed or covered if and when the original need for the creation of the area no longer exists (e.g., all classified material removed from the area for delivery to the customer).

d. To avoid confusion with restricted areas established on military installations for purposes other than the protection of classified material, Restricted Areas created in contractor facilities or activities located on such installations shall be designated "RESTRICTED AREA—AUTHORITY DoD MANUAL 5220.22-M."

34. Area Controls

a. Closed Areas.

- (1) Shall be separated from adjacent areas by a physical barrier capable of preventing unauthorized entry and, when visual access to classified material is a factor, observation by unauthorized persons. The physical barrier shall be substantially constructed of materials which provide protection against surreptitious entry or removal of classified material and which offers visual evidence of attempted surreptitious or forced entry (see Appendix V for construction criteria).

(2) During Working Hours.

- (*a*) Open or unlocked entrance. If the material within the area is classified no higher than CONFIDENTIAL, admittance shall be controlled by a properly

cleared contractor authorized employee or guard stationed so as to supervise the entrance to the area. If the material is classified SECRET or TOP SECRET, admittance shall be under the direct and continuous supervision of a properly cleared guard posted at the entrance.

- (b) Locked entrance. If the material within the area is classified no higher than SECRET, admittance shall be under the direct and continuous supervision of a properly cleared contractor authorized employee or guard, except as may be provided for by complying with paragraph 36. The employee or guard designated to control the entrance shall be required to unlock and open the entrance, remain at the entrance, while it remains open, supervise the passage of material or authorized personnel through the entrance, and to lock the entrance immediately thereafter. If the material is classified TOP SECRET, admittance shall be under the direct and continuous supervision of a properly cleared guard posted at the entrance.
- (3) During non-working hours admittance shall be controlled by locked entrances and exits, secured with either a built-in, three-position, dial-type, changeable combination lock, or a padlock as described in paragraph 14a(3)(d). However, doors secured from the inside with a panic bolt, a dead bolt, a rigid wood or metal bar, or other means approved by the cognizant security office, will not require additional locking devices. In addition, guards

on patrol shall be utilized, unless the contractor complies with the provisions of paragraph 35. The extent of such patrols shall be commensurate with the accessibility and size of the area, but as a minimum, the guard shall at all times be able to control ingress to and egress from the area, and to determine the presence of any unauthorized person.

- (4) Areas shall be designated and marked "Closed Area."
- (5) Employees assigned to the area shall challenge the presence of any unknown persons. The need-to-know principle shall be adhered to at all times within the Closed Area.

b. Restricted Area.

- (1) During working hours, the same controls as prescribed for Closed Areas during working hours.
- (2) During nonworking hours, the same controls as prescribed by paragraph 14.
- (3) Areas shall be designated and marked "Restricted Area."

c. Area Approval. The cognizant security office and the contractor shall agree upon the extent of the controlled area prior to the award of the contract, when possible, or at such subsequent times as the need for such areas become apparent during the performance on the contract. Where the costs of construction and/or maintenance of the controlled areas are to be charged against a User Agency contract, the cognizant security office shall obtain and furnish to the contractor written authorization from the contracting officer concerned for the expenditure of necessary funds. This authorization shall only be required when the contractor is performing on cost-reimbursement type

contracts as opposed to fixed-price type contracts in which such security costs would be included in the initial contract price.

d. Reports. The cognizant security office shall be advised in accordance with paragraph 6a(5) of the creation of any new controlled areas or of any change in the location of any existing controlled areas.

35. Supplemental or Supplanting Alarm Systems

a. Alarm systems may be divided into those that supplant the use of guards required under paragraph 34a(3), and those which supplement and extend the capability of guards.

- (1) When used to *supplant* guards, the electrical protective alarm system shall be connected to a central control station.

(a) The central control station may be located at the contractor's facility or at the facility of a subcontractor who maintains and operates the electrical protective alarm system and responds to alarms.^{2,3}

² A direct-connect or remote station alarm system (i.e., a system connected by direct wire to alarm receiving equipment located in a local police department headquarters, which is activated and deactivated by the using contractor and responded to by personnel of the local police department may be utilized when (i) the contractor's facility is located in an area where the central station services of a subcontractor are not available; (ii) it is impractical for the contractor to establish a proprietary or in-plant alarm system in accordance with the provisions of paragraph 35a(1)(c); (iii) the material and installation standards prescribed by paragraph 35b(1) or (2) are observed; (iv) response time to an activated alarm by local police personnel does not exceed 15 minutes from the time the alarm was first registered and arrangements shall have been made with the police department to immediately notify a representative of the contractor (preferably the facility security supervisor) upon receipt of an alarm; and (v) the representative of the contractor shall be required to report immediately to the facility to ascertain the nature of the alarm and to take appropriate measures to insure the security of the area concerned. Approval of the cognizant security office is required before a contractor may utilize a direct-connect system as an alternative to the use of a central station system. The proposed plan explaining how the system would operate should be submitted in duplicate to the cognizant security office, including sufficient justification for the granting of an exception and the full name and address of the police department which will monitor the system and provide required response. The name, address and clearance level of the subcontractor who installed the system and who will inspect, maintain and repair the equipment shall also be furnished, if applicable.

(b) Such a subcontractor and its employees shall have facility and personnel security clearances prescribed in paragraph 20e.

(c) Additional requirements for a central control station are:

1. Trained and appropriately cleared operators shall be in attendance at the central station at all times when the electrical protective alarm system is in operation. The device which signals alarms shall be continuously monitored.
2. Trained and appropriately cleared guards, sufficient in number to dispatch immediately a guard to investigate each alarm, shall be in attendance at the central station at all times when the electrical protective alarm system is in operation.
3. A signal shall be maintained at the central station to show whether or not the system is in working order and to indicate any tampering with the system. Necessary repairs shall be effected immediately.
4. Response time to an activated alarm (i.e., the time required for guards to reach the area) shall not exceed 15 minutes from the

³ Central station burglar alarm systems classified by the UL, Inc. as Grade A shall satisfy the requirements of this paragraph. Evidence of compliance with the UL standards may take the form of a UL Certificate or a letter issued by the installing company (see UL 611, Central Station Burglar Alarm Systems and list relating to authorized burglary protection equipment and installing companies in UL publication "Accident, Automotive, and Burglary Protection Equipment List").

DoD 5220.22-M

time the alarm was first registered.

5. Records shall be maintained indicating time of receipt of alarm, name of guards, time dispatched to area, time guards checked in, and nature of alarm. Such records shall be kept for a minimum of one year.
- (2) When used to *supplement* guards required by paragraph 34a(3), electrical protective alarm systems of the central station type, described in paragraph a(1) above, and systems not connected to a central control station may be used. However, if a central control station is not employed, the system shall provide an audible or visible alarm signal which shall be capable of attracting the immediate attention of guards on patrol in the area and directing them to the location of the alarm. In any event, the time required to respond to an activated alarm shall not exceed 15 minutes.
- (3) When such systems are used, they shall be activated immediately at the close of business.

b. Material and Installation Standards.

- (1) Where electrical protective systems are applied to an area to supplant or supplement guards, all material and equipment used in the system shall equal or exceed the standards prescribed in and shall be installed in accordance with (i) the provisions of Interim Federal Specification W—A—00450 “(GSA—FSS), Alarm Systems, Protective, Interior (Security), 3 November 1965”, or (ii) Underwriters’ Laboratories Standards for Intrusion-Detection Units, UL-639, and Underwriters’

Laboratories Standards for Installation, Classification and Certification of Burglar Alarm Systems, UL-681.^{4,5}

- (2) When individual alarms are installed on classified storage containers in accordance with paragraph 14a(2)(c) or 14a(4)(c), the installation shall provide “complete” protection of the top, bottom, sides and outer drawers or doors of the container (see Interim Federal Specification W—A—00450 and UL Standards 681 and 639). In addition, the requirements for a central station or direct-connect alarm system shall also apply (see paragraph a(1) above).

c. Approval by the cognizant security office is required before the installation of either a supplanting or supplemental alarm system to meet a requirement of this Manual (see paragraph 34c regarding cost considerations).

36. Supplanting and Supplemental Electronic, Mechanical, and Electro-Mechanical Access Control Devices

a. *Supplanting Devices.* Provided that the material within the controlled area is classified no higher than SECRET, electronic, mechanical, or electro-mechanical devices which meet the criteria stated below may be used to supplant contractor authorized employees or guards required under paragraph 34a(2)(b) to control admittance to the area during working hours.

- (1) Security enclosures (i.e., an enclosed metal booth, having an inner

⁴ The minimum required standard for installation on premises shall be Installation No. 3 (see UL-681). New installations shall conform to Interim Federal Specification W-A00450 to the maximum extent permitted by availability of qualified equipment.

⁵ Copies of the Interim Federal Specification may be obtained from any regional office of the GSA. Copies of the UL Standards may be obtained from Underwriters’ Laboratories, Inc., 207 East Ohio Street, Chicago, Illinois 60611.

and an outer door, inserted into an opening in the perimeter barrier for ingress to and egress from a controlled area. Access to the controlled area through the booth is restricted to authorized persons having knowledge of the combination on which the access control device is set to operate):

- (a) Control cards, if used in conjunction with the combination control panel, shall be rigidly controlled and accounted for by use of consecutive numbering system and promptly recovered upon termination or transfer of the holder to duties no longer requiring access to the controlled area involved. (Enclosures operated by a control card alone shall not be approved to supplant contractor authorized employees or guards required under paragraph 34a (2) (b).)
- (b) Possession of the combination on which the booth is set to operate and, if used, the control cards shall be limited to a minimum number of authorized personnel consistent with operational requirements.
- (c) The combination on which the booth is set to operate shall be classified in accordance with the classification of the highest classified material within the controlled area.
- (d) The selection and setting of the combination in the control panel shall be accomplished by an employee of the contractor who is authorized to enter the area in the performance of his duties, or by the facility security supervisor or his design-

nated representative who is authorized to enter the area. The combination shall be changed at least once every 3 months. The control panel shall be secured, by a three-position dial-type, changeable combination padlock as specified in paragraph 14a (3) (d).

- (e) Except as provided in paragraph b, below, the person entering or leaving the area through the security enclosure shall be responsible for insuring that the inner and outer doors are securely shut. In addition, only one authorized person may pass through the security enclosure at a time.
- (f) If an alternate entrance is used to transport bulky classified material to and from the area, a contractor authorized employee or guard shall be designated to unlock and open the entrance, remain at the entrance while it remains open, supervise the passage of the material and authorized personnel and lock it immediately thereafter.
- (g) During shift changes and emergency situations, when the fast exit switch in the control panel is set to allow both the inner and the outer doors of the booths to be opened at the same time, admittance shall be controlled by a contractor authorized employee or guard stationed so as to supervise the entrance to the area.
- (h) Electrical gear, wiring included, shall be accessible only from inside the area.

(2) Electronic, Mechanical, and Electro-Mechanical Door Devices (i.e., a system which operates by either a push-button combination which activates the locking device or by a control card used in conjunction with a push-button combination, thereby excluding any system which operates solely by the use of a control card.):

- (a) The control panel shall be installed in such a manner or have a shielding device mounted so that an unauthorized person in the immediate vicinity cannot observe the selection of the correct combination of the push buttons.
- (b) The electronic control box in which, or the mechanical mechanism by which the combination is set shall be secured by a three-position dial-type, changeable combination padlock as specified in paragraph 14a(3)(d), and shall be securely fastened or attached to the perimeter barrier of the area. To meet this requirement mechanical devices may be modified (e.g., by removal of the latching hold-back, addition of a hasp for securing the padlock to the backplate, and substitution of one-way screws).
- (c) The combination, and if also used, the control cards shall be

controlled in the manner prescribed by paragraphs (1)(a), (b), (c) and (d) above.

- (d) Authorized personnel entering or leaving the area shall be required to immediately lock the entrance behind them.
- (e) During shift changes and emergency situations, if the door remains open, admittance shall be controlled by a contractor authorized employee or guard stationed so as to supervise the entrance to the area.
- (f) In all cases when used, electrical gear, wiring included, or mechanical links (cables, rods, etc.) shall be accessible only from inside the area, or shall be secured within a protective covering to preclude surreptitious manipulation of such components.

b. Supplemental Devices. A number of electro-mechanical security devices for individual identification and authentication are currently available. These devices, such as those involving hand or fingerprint scanning and comparison, may be used to supplement the access control systems described in paragraphs a(1) and (2) above.

c. Approval. The approval by the cognizant security office is required before effecting the installation of either a supplanting or supplemental access control device to meet a requirement of this Manual (see paragraph 34c regarding cost considerations).

SECTION V

VISITOR CONTROL PROCEDURES

Part 1. VISITS TO USER AGENCY CONTRACTORS

37. General

a. The provisions of this Section, except paragraphs 45 and 48, apply only to persons who will have access to classified information. Access to information classified higher than the level in the visit authorization will not be granted regardless of the level of the visitor's personnel security clearance. The contractor or activity being visited shall take such security measures as may be required to preclude visitors from having unauthorized access to classified information. Nothing in this Section will limit the requirements of paragraph 5c.

b. The number of visitors requiring access to classified information shall be held to a minimum and the following requirements must be established:

- (1) That the visit is necessary.
- (2) That the purpose of the visit cannot be achieved without access to classified information by the visitor.

c. In the event the visit is disapproved, the requester shall be promptly notified by the contractor or activity which made the decision.

d. Requests for visits shall be furnished in writing (mail or teletype) to the contractor or User Agency activity being visited in advance of the proposed visit. In exceptional cases, the telephone may be used provided the visit request is confirmed in writing. Under no circumstances, however, may employees hand carry their own visit requests to the place being visited. All Category 1 and 2 visit requests shall contain the following information:

- (1) Name and address of the contractor or User Agency activity to be visited.
- (2) Name and title of person(s) to be visited, if known.
- (3) Name of the proposed visitor, his date and place of birth and citizenship. (If immigrant alien, so indicate.)
- (4) Job title or position of the proposed visitor.
- (5) Requesting contractor's or User Agency activity's certification of the level of clearance of the proposed visitor (see paragraph 38). If the clearance is an interim clearance, company CONFIDENTIAL or Canadian or U.K. Reciprocal clearance, so indicate (see paragraph e., below for Special Access requirements).
- (6) Purpose and justification for the visit, in detail, including contract, project or program under which the visit is necessary and identification of classified information to which access is required, if known.
- (7) Date or period during which the request is to be valid.
- (8) Name and address of the requesting contractor or User Agency activity.
- (9) Requesting contractor's certification of his facility security clearance (not required for representa-

→ tives of the U.S. Government) (see paragraph 38). If the contractor has a Canadian or U.K. Reciprocal facility clearance, so state.

- (10) Name, address and telephone number (if known) of requesting contractor's cognizant security office.

e. When visits involve access to classified information requiring a Special Access Authorization (e.g., CRYPTO, NATO, military space project or other special or limited access programs), the request will, in addition to the other required information:

- (1) Specify the program or project.
- (2) Specify the level of information to be released.
- (3) Certify that the visitor has been authorized access to such information.
- (4) Identify the office or User Agency activity granting such authorization.

→ f. When appropriate, the visit request shall ask for approval for subsequent visits within a 12-month period. The contractor or User Agency activity initiating the visit request shall immediately notify the contractor or activity being visited of any change in the visitor's status such as, the termination of employment, suspension, leave of absence, and the revocation or termination of clearance which will require the visit authorization to be cancelled prior to its normal termination date. In the event the initiating contractor's facility clearance, as indicated in paragraph d(9) above, changes to a Canadian or U.K. Reciprocal clearance, the initiating contractor shall immediately notify contractors or User Agencies honoring current visit requests so as to preclude the visitor's access to certain types of classified information as set forth in paragraph 31d. A downgrading of the facility security clearance also requires an immediate notification to contractors and User Agencies honoring current visit requests.

g. Machine-run or other rosters of employees, limited to those personnel who are authorized access to particular levels of classified information and who occupy positions which require classified visits, may be used for establishing visit request and approval authorizations as required by this Section, provided the machine-run (or other roster) or a covering letter furnishes the essential information required by paragraphs d, e, and f, above, and adequate procedures are in effect to notify the visited facility of changes in employee status which will affect his visit authorization. Use of such a procedures must be acceptable to the facility being visited and such records and control shall be maintained in a current status at all times.

h. Representatives of the following Government agencies, when acting in their official capacities, are not visitors.

- (1) Industrial Security Representatives of the DoD and other User Agencies.
- (2) Defense Investigative Service.
- (3) U.S. Army Intelligence Command. (Army)
- (4) Naval Investigative Service. (Navy)
- (5) U.S. Air Force, Office of Special Investigations. (Air Force)
- (6) Secret Service. (Treasury Department)
- (7) Federal Bureau of Investigation.

The contractor shall grant access to classified information to the minimum required upon presentation of proper credentials by the representative. In case of doubt as to identity or level of access authorized, such credentials and level of clearance will be verified by contact with the agency or activity concerned.

38. Identification and Control of Visitors

a. Contractors being visited by representatives of another contractor are responsible

for determining that the requesting contractor has been granted an appropriate facility security clearance, based either on an existing contractual relationship involving classified information of the same or higher category or otherwise by verification from the cognizant security office of the requesting contractor and certainly of the visitor's identity and authorization prior to any disclosure. When the requesting contractor's facility security clearance status has been determined, his certification as to the proposed visitor's personnel security clearance status may be accepted. If, however, there is any question as to the validity of a visit request or identity of the visitor, appropriate confirmation shall be obtained from the contractor or User Agency activity which initiated the visit request.

b. The contractor shall establish such controls over the movement of approved visitors as are necessary to insure that the visitors are only afforded access to classified information consistent with the authorized purpose of the visit. Particular care shall be taken to assure that his procedures for the control of Category 4 (foreign national) visitors are sufficient to prevent any access not provided for by the terms of the visit authorization. Such procedures shall provide for an escort while access is being afforded in accordance with the terms of the foreign national's visit authorization and when such a visitor is in areas where classified information may be accessible. The escort, when required, shall be a responsible, appropriately cleared employee who has been informed regarding the visitor's access limitations or restrictions on the visitor's movements.

c. Visitors shall be prohibited from making records of classified discussions or taking photographs in areas where classified information might be recorded on the film without the express permission of the contractor being visited.

d. Classified material shall not be released to the visitor to take outside the contractor's

facility except in accordance with other provisions of this Manual and specifically paragraphs 5*x* and 17.

39. Visitor Record

a. Except when the visitor is issued an identification card or badge in accordance with the provisions of paragraph 8*a*(7), the contractor shall maintain a record of all visitors to the facility for the purpose of having access to classified information. The record will indicate (i) the visitor's full name; (ii) the name of the contractor or activity he represents; and (iii) the date(s) of his arrival at and departure from the facility. A separate set of visitor records shall be maintained for NATO visitors in accordance with paragraph 54.

b. A NATO visit shall be considered to be (i) a visit by a person from a NATO country to a contractor in connection with pre-contract negotiations or contract performance on a NATO classified contract; (ii) a visit between a U.S. prime contractor and a subcontractor performing a NATO classified contract; and (iii) other visits in which access to NATO classified information has been specifically authorized. Representatives of the cognizant security office, whose requirement for access to NATO classified information is only incidental to the accomplishment of the security inspections at the contractor's facility, shall not be considered to be "NATO visitors" nor be required to enter their names on NATO visitor records.

c. The visitor record need not indicate whether the visitor actually did or did not gain access to classified information, but it must distinguish between classified and unclassified visits. Records of authorized visit requests for visits actually consummated shall be maintained by the contractor for a minimum of 2 years. Visit requests submitted in accordance with this Section may be retained in lieu of a visitor record if they also contain the information required in

CH 1

DoD 5220.22-M

items (i), (ii) and (iii) of paragraph a, above, and are retained for the required period.

40. Long-Term Visitors

When employees of one contractor are temporarily stationed at a facility of another contractor, the security procedures of the facility visited will govern. However, when such visits are on a continuing basis and it is found impractical for such visitors to comply with the security procedures of the host facility, the respective contractors shall prepare an agreement delineating their respective responsibilities and encompassing the procedures to be followed. This agreement must conform to the provisions of this Manual and a copy shall be furnished to the cognizant security office of the host contractor. The cognizant security office of the host contractor is responsible for conducting periodic inspections to insure that classified information in the possession of the visiting employees is properly safeguarded, and for notifying the host contractor of security deficiencies.

41. Visitor Categories and Procedures

a. *Category 1.* This category applies (i) where a contractual or prospective contractual relationship exists between contractors or between a contractor and a User Agency, and visits to a contractor by representatives of the GAO for auditing purposes, authorized representatives of the Department of Labor and other agencies of the Executive Branch of the Government when acting in their official capacities; (ii) to visits among prime contractors which are participating under Government direction in contracts pertaining to research, development or production of a weapon system (see paragraph 3bw); (iii) to employees of contractors producing items furnished to assembling contractors (GFP) for purposes pertaining to such assembly; and (iv) to employees of a cleared facility which had previously been furnished a classified report directly by the

contractor being visited under the specific terms of a contract (excluded from this category are facilities which receive only abstracts of classified reports or which receive reports from sources other than the preparing contractor). Such visit requests will, in addition to the information required in paragraph 37, also contain a statement identifying the specific report which the visitor is authorized to discuss.

- (1) The above visit requests will be submitted directly to the contractor to be visited.
- (2) The contractor to be visited has approval authority provided such visits meet the provisions of paragraph 37.
- (3) The prime contractor or assembling contractor, as the case may be, may initiate visit requests for employees of a subcontractor or contractors supplying GFP in accordance with paragraph 37 when he is in possession of the information required by paragraph 37d.
- (4) Employees of a temporary help supplier working for the contractor at his facility shall be treated as regular employees of the using contractor for the purpose of security orientation in facility practices, procedures and pertinent reports while working at his facility under his direction and control (see paragraphs 5u, v, ab, and 6b(1)). This action by the using contractor in no way relieves the temporary help supplier from complying with these and other requirements of this Manual.

b. *Category 2.* This category applies to visits between contractors who have been granted facility security clearances where a contractual relationship does not exist or which do not otherwise meet the requirements of Category 1.

- (1) The requesting contractor will ob-

tain in writing a verification of the visitor's need-to-know from his contracting officer and include it with the visit request.

- (2) The contractor to be visited will approve the request if he desires the visit.
- (3) The visiting contractor may substitute another cleared employee to make the visit without additional verification of the need-to-know if acceptable to the contractor being visited. Information about the substitution shall be furnished the contractor being visited as required in paragraph 37d.

c. Category 3. Representatives or employees of the ERDA and its contractors whose visits require access to other than RESTRICTED DATA.

- (1) The activity requesting the visit will furnish the required information to the contracting officer of the User Agency whose information is involved, using ERDA Form 277.
- (2) If approved, the contracting officer will notify the contractor of the scheduled visit including required information concerning the visit (ERDA Form 277).

d. Category 4. Foreign Nationals (see paragraph 3ae). Visits by foreign nationals will not normally involve access to classified information and may be arranged directly between the foreign activity proposing the visit and the contractor to be visited. The contractor shall be responsible for insuring that such visitors are effectively denied access to classified information in the facility's possession and to unclassified technical data on the U.S. Munitions List for which an export license or letter has not been issued by the State Department under the ITAR or other unclassified information for which

the Government has prescribed dissemination limitations. In those cases when the foreign activity has requested a User Agency's approval for the visit and the visit has been approved on an unclassified basis, the User Agency will advise the contractor that the foreign activity has been authorized to contact the contractor directly to arrange the visit. In the latter case an export license or letter is not required.

- (1) Foreign nationals shall not be afforded access to classified information unless specifically authorized in writing by the User Agency (U.S. host military department).
- (2) The User Agency (host military department) will send the visit authorization which will contain the level and scope of classified information to be released (visual and/or oral only) as well as any other limitations, to the contractor facility to be visited through the cognizant security office. The contractor will notify the User Agency (host military department) whether or not the visit is desired. When the purpose of the visit cannot be accomplished without upgrading the level and scope of classified information authorized for release, or without modifying other limitations, the contractor will so advise the User Agency (host military department). The contractor will not advise the foreign government concerned, or its representative of the level or scope of access authorized by the User Agency (host military department), nor will the foreign government or its representative be induced to seek a higher access level than that previously approved by the User Agency (host military department).

- (3) An export license is not required to release unclassified technical data

DoD 5220.22-M

covered by the ITAR for visits approved as in paragraph (2), above, unless prohibited by the visit request.

- (4) Prior to disclosure to visitors in this category, the contractor being visited shall advise the visitor of his continuing responsibility to safeguard the information to be disclosed. He shall also inform him that the information affects the national defense of the U.S. within the meaning of the espionage laws of the U.S., that unauthorized disclosure violates international agreements and is inimical to the interests of national security.

e. Category 5. This is a miscellaneous category which is used only if Categories 1 through 4 do not apply. Justification for this category of visit must be approved by the cognizant security office. Thereafter, individuals making Category 5 visits must be authorized by DISCO.

- (1) Persons, other than employees of the contractor, whose visit is considered necessary by the contractor and who cannot be denied some degree of access to classified information by escort or other procedures because of the nature of their presence in the area. The contractor to be visited will furnish the cognizant security office the following information:

- (a) The information specified in paragraphs 37d(1), (2), (3), (4) and (7).
- (b) Justification for the visit and the reason access to classified information cannot be prevented. Interim visit approval, based on requirements for interim clearance as set forth in paragraph 26d, is authorized in emergency situations so as to avoid crucial

delays in the fulfillment of contractual obligations.

- (c) Personnel security clearance forms specified in paragraph 26. Contractors to be visited will act as sponsors instead of employers in the completion of the clearance forms.

- (2) If the cognizant security office disapproves the request, it shall so advise the contractor. If the cognizant security office approves the need and justification for access to classified information, it will forward the request to DISCO, which will notify the contractor of the authorization or disapproval of the visit. A DISCO Form 560 shall not be used.

- (3) Category 5 visits are normally authorized for one-time visits only, but may be approved by the cognizant security office for periods up to 1 year, when justified. Such visit authorizations may be renewed by forwarding a request to the cognizant security office with appropriate justification for the renewal and the information specified in paragraphs 37d(1), (2), (3), (4) and (7). When the requirement for a Category 5 visit authorization ceases to exist prior to expiration of the period for which it is valid, notice of termination shall be provided to DISCO by forwarding one copy of the DLA Form 562-R, annotated in the "Remarks" section to reflect the action taken. The sponsoring contractor being visited shall handle the briefing, debriefing, reporting, and other provisions of this Manual as he would for his own employees.

42. Visits Involving Access to RESTRICTED DATA

- a.* Visits to a DoD or NASA contractor by a DoD or NASA representative or contrac-

tor shall be processed as prescribed in paragraph 37.

b. Visits to a DoD or NASA contractor by representatives of User Agencies other than DoD and NASA and their contractors require prior approval of the ERDA. The ERDA visit request form (ERDA Form 277) shall reflect this approval in Part B of the form. Contractors submitting visit requests in this category shall, after certifying to the clearance status of the proposed visitor(s) in Part A of the ERDA Form 277, forward the form to the contracting officer for certification of the visitor's need-to-know and further processing in accordance with the User Agency's regulations. The contractor receiving a visit request in this category shall insure that the required certifications

have been made and that the visit has received ERDA approval.

c. Visits to a User Agency contractor, other than to a DoD or NASA contractor by representatives of the contracting User Agency and between a prime contractor and his subcontractor on such a User Agency contract, shall be processed as prescribed in paragraph 41.

d. Visits to a User Agency contractor, other than to a DoD or NASA contractor, by representatives of User Agencies other than the contracting User Agency and by contractors other than under a prime-subcontract relationship require prior approval of the ERDA and shall be processed in the manner prescribed in paragraph *b*, above.

Part 2. VISITS TO USER AGENCY ACTIVITIES

43. General Rules—In addition to paragraph 37

a. Contractors shall comply with any requests received from the Commander or Head of User Agency activities for additional information needed in the processing of visit requests.

b. The contractor is encouraged at the time of the initial visit to request approval for subsequent visits within a period of twelve months, when necessary and consistent with the purpose of the initial visit. Arrangements for continuing visits will be made between the contractor and the Commander or Head of the User Agency activity. Final approval is the prerogative of the Commander or Head of the User Agency activity.

c. Visits to DoD or NASA activities by DoD or NASA contractors involving access to RESTRICTED DATA shall be processed as prescribed in paragraph 42a. Visits to other User Agencies involving access to RESTRICTED DATA shall be processed in the manner prescribed in paragraph 42b.

d. Contractor employees shall comply with written regulations and operating instructions issued by User Agency activities concerning visitors to such activities.

44. Visits to User Agency Activities in the U.S.

a. *Visits to Field Activities.* Contractors desiring to have an employee or consultant visit a User Agency activity involving access to classified information shall address a request in writing to the Commander or Head of the activity to be visited. Visit requests shall be accompanied by a statement from the contracting officer that the release of classified information is required in connection with a specified classified contract or program. (Visit request normally will be sent via the contracting officer.)

b. *Visits to User Agency Activities in the Washington, D.C. Area.* Requests to visit offices of headquarters activities of the User Agencies in the Washington, D.C., area shall be submitted in writing addressed to the specific office to be visited. Whenever possible, the exact code number, division, branch, etc., of the activity or office to be visited shall be included in the address of the request. Visit requests shall be accompanied by a statement from the contracting officer that the release of classified information is required in connection with a specified classified contract or program. (Visit requests normally will be sent via the contracting officer.)

c. As an exception to paragraphs a, and b, above, a visit request may be submitted directly to the activity or office to be visited without a statement from the contracting officer when the classified information to be disclosed and the determination as to the contractor's need for such access is known to be a responsibility of the activity or office to be visited. This exception does not apply to visits involving access to classified intelligence information as set forth in paragraph e, below.

d. The contractor's request shall contain the information specified in paragraph 37d.

e. If a contractor contemplates discussion or viewing of classified intelligence in the custody of a User Agency activity, the contractor's visit request shall be forwarded in all cases to the contracting officer of the User Agency activity authorized to release classified intelligence to contractors for the required need-to-know verification and routing to the User Agency to be visited. In addition to the information specified in paragraph 37d, the visit request shall contain:

- (1) The contractor's certification that
 - (i) access to classified intelligence is required for contract perform-

ance and (ii) the contract is a classified contract (see paragraph 3f).

- (2) Sufficient additional information concerning classified intelligence required to permit the agency or activity receiving the visit request to assess:

- (a) Applicability of available classified intelligence to the contractor's needs.

- (b) Whether available intelligence may be released to the contractor without permission of the originator and/or sanitization of the material.

45. Visits to User Agency Activities Outside the U.S.

This paragraph is applicable when a contractor desires to have an employee make a classified or unclassified visit to a User Agency activity outside the U.S. The information required by paragraph 37d shall be furnished for the visits enumerated in this paragraph.

a. Contractor Sponsored Visits. A contractor shall process a request for his employee to visit a User Agency activity outside the U.S. through DISCO to the User Agency activity concerned if the visit is on the initiative of the contractor. The Commander or Head of the activity to be visited will notify the contractor of the approval or disapproval of the visit request. (See paragraph 50 for an employee based in Europe.)

b. User Agency Sponsored Visits. A visit request for a contractor employee sponsored by a User Agency other than under a DCAS administered contract and traveling on the User Agency's orders, will be processed by the User Agency in accordance with the regulations of such agency. The traveler's orders shall reflect the traveler's level of security clearance, if required, in connection with the travel. The contractor shall submit the request for such visit directly to the User Agency activity concerned.

c. Visits Under DCAS Administered Contracts. A visit in this category shall be processed concurrently to DISCO and the ACO at the DCASR as early as possible. For advance notice or lead time see paragraph 49.

- (1) DISCO shall request visit authorization and verify the contractor employee's personnel security clearance to the overseas activity or advise the activity that the employee does not have a clearance. The DISCO shall request the overseas activity to forward approval or disapproval of the visit request to the ACO at the DCASR.

- (2) Concurrent with the processing of the visit request to DISCO, the contractor shall execute Part I of Request and Authorization for Overseas Travel—Contractor Personnel (DLA Form 437) in duplicate and forward it to the ACO at the DCASR. The contractor will be advised of the approval or disapproval of the visit by the ACO. (Copies of DLA Form 437 shall be obtained from the DCASR.)

Part 3. VISITS TO GOVERNMENT ACTIVITIES OTHER THAN USER AGENCIES

46. Visits to ERDA Installations or ERDA Contractors

Requests for visits to ERDA installations or to ERDA contractors which will require

access to ERDA classified information shall be prepared utilizing ERDA Form 277. (Copies of this form may be obtained from any ERDA installation.) In addition to completing the appropriate portions of the

ERDA Form 277, the contractor (usually the facility security supervisor) shall include, in the first block of the form immediately after the personnel clearance data, a certification of the prospective visitor's personnel security clearance. The ERDA Form 277 shall then be forwarded for the required official certification to the contracting officer of the User Agency who signed the DD Form 254 which was issued in connection with the contract for which the ERDA classified information is required.

47. Visits to Activities Other Than ERDA

Requests for visits to Government activities, other than User Agencies and the ERDA which involve the release of classified information to such activities in connection

with a User Agency contract, require the approval of the contracting officer and, if the classified information to be released includes RESTRICTED DATA, the approval of the ERDA. Such requests shall be submitted by the contractor to his contracting officer who will process to request. The contractor shall provide evidence of the fact that the activity to be visited had either requested the proposed visit or else consented to the contractor's request for the visit. In addition, a statement shall be included explaining: (i) the purpose of the visit in detail; (ii) a description of the classified information to be divulged during the visit, either to or by the activity being visited; and (iii) the direct or indirect effect the visit may have on the performance of the classified contract involved.

Part 4. VISITS TO FOREIGN GOVERNMENTS AND ACTIVITIES

48. General

a. Contractor visits to foreign governments or activities or to international bodies fall into three categories:

(1) Visits which involve the disclosure of U.S. classified information:

(a) In connection with a government-to-government agreement to furnish U.S. military equipment to the foreign government (i.e., the purchase of the equipment is under a U.S., not a foreign government contract); or

(b) In connection with exploratory sales visits, precontract negotiations or contract performance, other than those covered under paragraph (a) above (i.e., the purchase of the U.S. military equipment or services when and if consummated will be or is under a

foreign government contract); or

(c) In connection with U.S. Government presentations to foreign governments and international pact organizations when the U.S. Government has requested the contractor's participation.

(2) Visits which do not involve disclosure of U.S. classified information but where the foreign government or activity requires a U.S. security assurance on the visitor:

(a) Which involve disclosure of unclassified technical data on the U.S. Munitions List; or

(b) Which will not involve disclosure of technical data on the U.S. Munitions List.

(3) Visits on a commercial basis (i.e., do not involve disclosure of U.S.

classified information and do not require a U.S. security assurance on the visitor). These visits may or may not involve disclosure of unclassified data on the U.S. Munitions List. Visits in this category are not processed under the provisions of this Manual. However, the contractor is responsible for compliance with the ITAR and for obtaining a State Department export license or letter, if required.

b. The following information concerning the requirements of the ITAR is furnished for the guidance of the contractor:

- (1) Disclosure of classified information in connection with visits in the category described in paragraphs a(1)(a) and (c) above does not require an export license.
- (2) Except as specified in paragraph (3) below, disclosure of unclassified technical data related to U.S. Munitions List items requires an export license.
- (3) An export license is not required if the visit has been approved on an unclassified basis by the User Agency concerned, and (i) the technical data to be disclosed is information covered by a manufacturing license or technical assistance agreement approved by the Department of State, or (ii) the technical data to be disclosed is exempt from the provisions of the ITAR.

c. Requests for visits to foreign governments or activities shall be processed only for an employee who is the subject of a Letter of Consent. Contractor issued CONFIDENTIAL clearances are not valid for such visits.

d. Visit requests shall be processed as follows:

- (1) Visit requests in the categories described in paragraphs a(1)(b) and a(2)(a) and (b) above shall be processed by the contractor through DISCO.
- (2) Visits in the categories described in paragraphs a(1)(a) and (c) above shall be processed by the contractor in accordance with the regulations of the User Agency which is dealing with the foreign government. The contractor shall certify visit clearance information directly to the User Agency concerned. Such visits are not processed through DISCO.

e. Visit requests processed through DISCO shall be submitted in duplicate with one extra copy for each additional country to be visited, and shall contain the information required in paragraph 37d, as well as proposed visitor's passport or identification card number, date and place of issue. In addition, the contractor shall specify the category of visit which is involved (see paragraph a, above) and, for a visit of the type described in paragraphs a(1)(b) or a(2)(a) above shall enclose a copy of his export license or letter. For visits to the Swiss Government and contractor facilities, the legal residence address of each visitor must also be shown.

49. Processing Time

Visit requests should be received by DISCO at least 30 days in advance of the proposed travel date for all countries and U.S. overseas Commands. Exceptions are travel to Switzerland, which requires 49 days advance notice; and the following, which normally can be processed in less than 30 days:

Belgium	21 days
Canada	10 days
France	21 days
(France will not accept visits for 6	

months. It will accept visits only for specific dates.)

Netherlands	21 days
United Kingdom	
Ministry of Defense	21 days
Ministry of Technology	16 days
Royal Navy	28 days

50. Use of OISE

If the U.S. contractor employee making the visit is based in Europe, or in an ad-

jacent non-European country, the visit request may be submitted through OISE rather than through DISCO. The information required in paragraph 48e shall be included with the request. The OISE will verify the proposed visitor's security status. In addition to furnishing a copy of the export license or letter, when required in accordance with paragraph 48e, the contractor is responsible for compliance with the ITAR, if applicable, in the same manner as though the visit were arranged through DISCO.

Part 5. VISITS IN CONNECTION WITH BILATERAL INDUSTRIAL SECURITY AGREEMENTS AND NATO VISIT PROCEDURES

51. Visits in Connection With Bilateral Industrial Security Agreements

a. The following procedures apply to visits pertaining to precontract negotiations or contract performance under approved bilateral agreements involving a foreign classified contract in the U.S. or a U.S. classified contract in a foreign country.

- (1) Authorization for visitors or those visited to have access to classified information shall be limited to that necessary for official purposes in connection with precontract negotiations or contract performance. When requested, the authority to visit the facility of the prime contractor may include authorization to have access to or to disclose classified information at the facility of a subcontractor engaged in performance of work in connection with the same contract.
- (2) A list may be developed to indicate those individuals who are authorized to visit the facility for extended periods of time, not to exceed six months, as may be necessary in the performance of the contract. This authorization may be renewed for additional periods of 6

months as may be necessary in the performance of the contract.

- (3) Visits shall be approved only for persons possessing Government granted security clearances.

b. U.S. contractor visits in connection with foreign classified contracts shall be processed in accordance with the provisions of paragraph 48.

c. Representatives of foreign governments visiting U.S. activities shall be processed as Category 4 visitors in accordance with paragraph 41d if the U.S. classified information is involved in the foreign government's contract. If only foreign classified information is involved, the visit shall be processed by DISCO.

52. NATO Visit Procedures

The following visitor control procedures apply to a NATO precontract negotiation or to a NATO contract awarded to a U.S. contractor by a NATO government other than the U.S., a contractor of such NATO country, or a NATO international body.

a. Visits by Representatives of a U.S. Contractor to the NATO Contracting Officer,

a NATO Management Office or a Contractor of a NATO Country Other Than the U.S. The visit request, in quadruplicate, will be directed through DISCO to the NATO contracting office or to the NATO management office and will be processed together with a Certificate of Security Clearance (see paragraph 55). The Certificate of Security Clearance shall indicate whether or not the visitor has received a NATO security briefing. Whenever possible, the NATO security briefing will be accomplished prior to the submission of the visit request and the certificate will so state. When this is not practical, the visit request will include a statement as to when and by whom the NATO security briefing will be conducted. The visit request shall include the information specified in paragraph 37d, the visitor's passport or identity card number, date and place of issue and the NATO contract or program on which he is engaged.

b. Visits by Representatives of NATO Contracting Officer, a NATO Management Office, or of a Contractor of a NATO Country to the U.S. Contractor. Such requests shall be processed by the NATO activity concerned as a Category 4 visit (see paragraph 41d) through the appropriate User Agency activity. Such visit requests will contain the information specified in paragraph a, above.

c. Visits in Connection with NATO Contracts by Representatives of a U.S. Contractor to Another U.S. Contractor in the U.S.

- (1) Such visits shall be processed as Category 1 visits (see paragraph 41a) if both contractors are performing on the same NATO contract in a prime contractor to subcontractor or subcontractor to subcontractor relationship. A statement on NATO security briefing shall be included in the visit request.
- (2) If no contractual relationship exists between the contractors, the visit

request shall be processed as a Category 2 visit (see paragraph 41b) requiring the approval of the NATO contracting officer whose information is involved. Supporting information on NATO briefing and Certificate of Security Clearance shall be included in such visit requests. The visit request, together with two copies of Certificate of Security Clearance, will be processed through DISCO to the NATO Contracting Officer.

d. Recurring Visits. Subsequent visits shall be processed in accordance with paragraph 37f. Authorization for subsequent visits shall not exceed a period of 12 months, but may be subject to renewal for succeeding periods of 12 months, if required (see paragraph 53b for NPLO visit requests).

53. NPLO Programs Clearance and Visit Procedures

Clearance and visit control procedures in effect for contractors performing on specific NPLO programs are different from other NATO visit procedures. Current, NPLO programs are HAWK, F-104G, NAMSA, and NISCO. As an aid to simplifying visit procedures, it is necessary to establish the visiting contractor employee's clearance in connection with a specific NPLO program. This may be accomplished prior to the initial visit or concurrently with the request for such visit.

a. Initial Visits.

- (1) The visit request, in quadruplicate, will be directed through DISCO to the NPLO Management Office with a copy to the NATO activity to be visited and will be processed together with a Certificate of Security Clearance (see paragraph 55). The visit request shall include the information specified in paragraph

37d, the visitor's passport or identity card number, date and place of issue, and the NPLO program with which he is concerned.

- (2) The DISCO will forward the visit request to the Management Office of the NPLO which will inform appropriate NATO and foreign activities of its action; i.e., approval or disapproval.
- (3) The Certificate of Security Clearance will be forwarded by DISCO to the NATO Office of Security, Industrial Security Section, for recording and dissemination of the information to the NATO member countries and NPLO Management Offices concerned.
- (4) In case of urgency when a Certificate of Security Clearance has not been forwarded to the NATO Office of Security, Industrial Security Section, in advance, DISCO will attach a copy of the Certificate of Security Clearance to the visit request for onward transmission to the NPLO Management Office.

b. Recurring Visits. If the initial visit is approved, subsequent visits, not to exceed 6 months to the same NPLO activity for the same U.S. contractor employee will be processed by the U.S. contractor directly to the NPLO activity to be visited. That activity will notify the contractor of the approval of the visit. These subsequent visit requests will contain the information required by paragraph 37d and will include the visitor's passport or identity card number, date and place of issue.

54. Records of NATO Visits

The contractor shall keep a separate set of visitor records for NATO visitors containing the information specified in paragraph 39.

55. Certificate of Security Clearance

a. A standard format Certificate of Security Clearance has been adopted for use within the NATO community in connection with visits from one NATO country to another, or to a NATO office, agency, command or to or between contractors when a visit will involve access to NATO classified information.

b. The Certificate of Security Clearance shall be completed on plain bond paper by the contractor for his employees desiring to make a visit, and submitted in duplicate for certification to DISCO. The employee's name shall be listed in the following order: last name, first name, middle name.

c. This certificate shall be sent sufficiently in advance by the contractor through DISCO so as to assure receipt by the foreign officials of the NATO offices, agencies, commands, or contractors before arrival. In exceptional circumstances, the information required by the certificate may be supplied by other means of communication but must be confirmed in writing. Normally a copy of this certificate should not be given the traveler.

DEFENSE INDUSTRIAL SECURITY
CLEARANCE OFFICE
DEFENSE LOGISTICS AGENCY

Certificate of Security Clearance

(Authorizing access to NATO Classified Information)

Issued by _____

Data and place of issue _____

Valid until _____

(If issued to an individual this certificate should be returned to the granting authority on the termination of the mission for which issued)

This to certify that _____
Last name, first name, middle name

Date of birth _____

Place of birth _____

Nationality _____

Where employed _____

Programme(s) _____

Holder of passport/identity card No. _____

Issued at _____

Military rank and number _____

_____ (where applicable)

has been cleared for access to information clas-
sified up to and including _____ in

accordance with current NATO Security Regu-
lations.

(Has) (Has not) received a NATO Security
briefing.

Signature and title of granting Authority
(seal or stamp)

SECTION VI

SUBCONTRACTORS, VENDORS AND SUPPLIERS

56. Application to Subcontractors

The provisions of this Manual apply to subcontractors, vendors or suppliers of prime contractors (hereinafter referred to as a subcontractor). A subcontractor shall submit requests through the prime contractor to the contracting officer for an authorization or approval requiring action by the contracting officer under the provisions of this Manual. However, if any such request is clearly encompassed in an authorization previously given in writing to the prime contractor by the contracting officer in relation to a specific contract, the prime contractor, acting within the scope of such authorization, may approve or disapprove such request. Requests involving release of U.S. classified information to foreign subcontractors must be forwarded to the User Agency for authorization.

57. Application to Sub-Contractors

For the purposes of this Manual, each subcontractor shall be considered as a prime contractor in relation to his subcontractors.

58. Determination of Clearance Status

a. The prime contractor shall determine from the cognizant security office of the prospective subcontractor that the prospective subcontractor has been granted an appropriate facility security clearance prior to disclosure of any classified information, unless there is an existing contractual relationship between the parties involving classified information of the same or higher category. (A facility security clearance is not prima facie evidence that a facility has the capability to physically safeguard classified ma-

terial.) If physical possession of any classified material is to be granted to the prospective subcontractor, the procedures outlined in paragraph 59 shall be followed.

b. If the prospective subcontractor does not have an appropriate facility security clearance, the prime contractor may request the cognizant security office over the geographic area in which the subcontractor is located to initiate clearance action.

59. Safeguarding Ability

a. Prime contractors having complied with paragraph 58a, shall obtain written approval from the contracting officer or his designated representative prior to the disclosure of TOP SECRET information to prospective subcontractors.

b. Prime contractors, having complied with paragraph 58a, shall determine that prospective subcontractors meet the requirements of this Manual for safeguarding TOP SECRET, SECRET, and CONFIDENTIAL material prior to granting physical possession of such material to prospective subcontractors. (This determination may be made at the same time as the facility clearance determination is made under paragraph 58a.) Such determination shall be based on:

- (1) The prime contractor's knowledge of the ability of the prospective subcontractor to safeguard adequately the material to be released and produced under the subcontract based upon a current contractual relationship involving classified material of the same or higher cate-

gory as that to be released or produced under the new subcontract; or

- (2) The written authorization of the cognizant security office of the prospective subcontractor. In this connection, the prime contractor shall furnish the cognizant security office of the prospective subcontractor, information available to him, such as description, quantity, end-item, and classification of information related to the proposed subcontract and any other factors, in order to assist the cognizant security office in determining whether the prospective subcontractor meets the safeguarding requirements of this Manual.
- (3) The cognizant security office of the prospective subcontractor shall advise the prime contractor in writing that the prospective subcontractor is or is not physically equipped to safeguard the classified material involved. When necessary action is taken by the prospective subcontractor to provide adequate safeguards, the cognizant security office of the prospective subcontractor shall immediately inform the prime contractor.
- (4) In exceptional cases, where the situation dictates, the data required by this paragraph and paragraph 58 may be furnished by telephone or other rapid means of communication, provided the request and substantiating facts are confirmed later in writing.
- (5) Clearance status and safeguarding capabilities of facilities shall be obtained only when a specific procurement need exists. A compilation or indices of such information for possible future use shall be prohibited.

60. Classification Guidance

a. Prime contractors have a requirement to inform prospective subcontractors of the category of classification to be assigned the various elements in a subcontract, RFQ, RFP, IFB or other solicitation. The prime contractor in preparing the DD Form 254 for his subcontracts may extract pertinent data from the DD Form 254 pertaining to the prime contract. The DD Form 254 prepared by the prime contractor shall be submitted to the official shown in item 16e of the prime contract DD Form 254 for approval and distribution or authorization and instructions for distribution by the prime contractor. In the absence of exceptional circumstances which clearly support classification, the DD Form 254 will not be classified. If classified supplements are required as part of the security classification, they shall be identified in item 15 of the DD Form 254 and forwarded in separate correspondence. Classified information shall be so furnished after verifying clearance status and safeguarding ability in compliance with paragraphs 58 and 59. The provisions of this paragraph do not waive the requirements of paragraph 62.

b. After selection of a subcontractor, the prime contractor shall prepare a DD Form 254 for the subcontract and shall request the official designated in item 16e of the DD Form 254 for the prime contract to approve and sign the DD Form 254 for the subcontract and to make the required distribution. However, with the agreement of the contract activity, the prime contractor may accomplish the required distribution of the approved DD Form 254. The distribution schedule of the DD Form 254 is included as paragraph 61.

c. When the prime contractor receives a *revised* DD Form 254 providing additional guidance or a change in guidance, he shall prepare a *revised* DD Form 254 for each

subcontractor whose DD Form 254 requires a related change. An ACO/PCO authenticating signature, and distribution or instructions for distribution of the contractor's DD Form 254, are required. When the prime contractor receives notice that a review has reaffirmed his existing guidance, or receives a *revised* DD Form 254 that does not require a related change in any subcontractor's DD Form 254, he shall promptly give written notice of reaffirmation of guidance to each subcontractor involved. This notice of reaffirmation to subcontractors does not require ACO/PCO authenticating guidance. Instead, a true copy of the notice of reaffirmation received by the prime contractor, or, when applicable, a true copy of pages 1 and 2 of the *revised* DD Form 254 received by the prime contractor, annotated by the prime contractor with the statement "This *revised* DD Form 254 does not affect your current DD Form 254 dated, " in either case attached to a signed transmittal letter from the prime contractor, will suffice. Distribution of this written notice of reaffirmation to subcontractors shall be in accordance with paragraph b., above. With respect to a multiple facility organization, the home office shall provide the *revised* guidance, or the written notice of reaffirmation of existing guidance, above described, as applicable, to each of its operating facilities affected by the *revised* guidance or involved in the notice, as the case may be.

d. The prime contractor will receive from the User Agency a DD Form 254 for each classified item of GFP or GFE issued or authorized for purchase when such material is not covered by the classification specification issued with the contract. The contractor shall furnish a DD Form 254 providing the classification specification necessary for each subcontractor requiring use of classified GFP of GFE in connection with their contracts or negotiations for contracts with the prime contractor.

e. A new DD Form 254 is not required for a follow-on contract or subcontract when the

procurement is of a recurring nature or the end item is not changed and there is no change in the security classification requirements of the contract. However, a copy of the currently valid DD Form 254 for the preceding subcontract shall be furnished and distributed with the follow-on subcontract and annotated in items 3 and 4 to show the contract number and date of the follow-on prime and subcontract. Item 6 will also be completed, as appropriate.

f. There is no authorized substitute for the DD Form 254. There are exceptional conditions in which a prime contractor has a serious time limitation in preparing his response to a request for proposal, invitation for bid, or similar solicitation to a User Agency. In such cases the prime contractor, concurrent with dispatching the DD Form 254 for official Government approval and signature, may supply an unofficial copy of the same guidance to a prospective subcontractor for the latter's use pending receipt of the approved and signed DD Form 254.

g. A single DD Form 254 may be used to provide the classification specification for an open-end or call-type subcontract except when the individual call, purchase order or request for services or products requires a different classification specification from that provided for the overall subcontract.

h. The following special provisions are applicable to service, graphic arts, research, or commercial carrier classified contracts:

(1) A DD Form 254 which specifies the highest level of classification involved, but *does* not provide detailed classification guidance, will be issued when:

(a) The total requirement of the contract is the performance of a service, all of which takes place at a cleared contractor's facility or Government activity which has and makes available, for use by the contractor per-

forming the service, a currently valid Contract Security Classification Specification which includes complete guidance for the service to be performed. In such cases, item 15 of the DD Form 254 will be annotated "Using contractor or activity will furnish complete classification guidance for the service to be performed. The highest level of classification for the contract is (*TOP SECRET, SECRET, or CONFIDENTIAL*). Contract performance is restricted to (*name of facility or location*)."

- (b) The contractor has no performance requirement involving actual knowledge of, generation or production of classified information, but has only a requirement to be physically present in an area where classified information is located. Examples include, but are not limited to, contracts calling for guard, alarm, alternate storage, or equipment maintenance services. In these cases, item 15 of the DD Form 254 will be annotated "Actual knowledge of, generation, or production of classified information NOT REQUIRED. This document serves as written notice of the letting of a classified service contract. The highest level of classification for the contract is (*TOP SECRET, SECRET, or CONFIDENTIAL*)."
- (c) The contract requirement is limited to graphic arts reproduction and classification markings appear on the ma-

terial to be reproduced. These classification markings constitute the required Contract Security Classification Specification. In these cases, item 15 of the DD Form 254 will be annotated "Reproduction service only. The highest level of classification for the contract is (*TOP SECRET, SECRET, or CONFIDENTIAL*). Classification markings on material to be reproduced specify the required security classification."

- (2) Where a cleared commercial carrier enters into a classified service subcontract with a cleared facility, within the meaning of paragraph (1)(b) above, the carrier, serving as a prime contractor for such purpose, will issue a DD Form 254 to that cleared facility. In any such case, the requirements of paragraphs (1)(b) above, and (3) below, will apply.
- (3) In each of the cases described in paragraphs (1) and (2) above, if a subcontract at any tier is involved, the DD Form 254 for the subcontract will *not* require authentication by the signature of an ACO/PCO. Instead, the contractor who is the principal prime, or who serves as a prime in relation to a sub in the particular case, will complete and sign item 16. Further, in all cases distribution of the DD Form 254 will be made to the subcontractor involved, his cognizant security office, and the contract administration office(s), if designated, of the immediate prime and subcontractor involved.
- (4) Where a contract involves research services requiring detailed classification guidance, but it is too early

to determine these detailed requirements, item 15 of the DD Form 254 will be annotated "This is a *research* contract. The highest level of classification for the contract as a whole is (*TOP SECRET, SECRET, or CONFIDENTIAL*). A revised DD Form 254 will be issued as soon as possible to provide detailed security classification guidance."

i. In the case of a subcontract which is expected to require access only to classified reference material (see paragraph 3a) an *original* DD Form 254 will be issued to describe the highest category or various categories of classification of such material to which access will be required and to provide other instructions, as appropriate, for example, the protection of information extracted from such material. Classification guidance concerning reference material over which the User Agency which awarded the prime contract does not have classification jurisdiction, is the responsibility of the DoD component having classification jurisdiction over such material at the time it was prepared, or of the current successor in interest of that component. When the prime contractor requires clarification of the classification specification regarding reference material in order to prepare a DD Form 254 for the subcontractor, or for other reasons, and desires assistance in identifying the responsible DoD component, he shall, by direct communication, seek assistance from:

- (1) The secondary distribution source from which the material was received. Examples of secondary distribution sources are: DDC, Alexandria, Virginia 22314 and its field extensions; DoD Information Analysis Centers; and the Redstone Scientific Information Center, U.S. Army Missile Command, Redstone Arsenal, Alabama 35808.

- (2) The User Agency contracting office

last involved with the contractor concerning the subject matter of the material.

- (3) The DASD (SP).

61. Required Distribution

Original, Final and Revised DD Forms 254, supplements, attachments, and written confirmation of existing classification specifications are to be distributed as follows:¹

- a. For prime contracts:

- (1) Prime contractor.
- (2) Cognizant security office of prime contractor only.
- (3) Appropriate ACO.
- (4) Quality assurance representative.
- (5) Official identified in item 12b, DD Form 254.
- (6) Others as necessary.

- b. For subcontracts:

- (1) Prime contractor.
- (2) Appropriate ACO.
- (3) Subcontractor.
- (4) Cognizant security office of subcontractor only.
- (5) Quality assurance representative.
- (6) Official identified in Item 12b, DD Form 254.
- (7) Others as necessary.

¹ Reflect the distribution of the "Required Distribution" block of the DD Form 254. For SENSITIVE COMPARTMENTED INFORMATION contracts, distribution of the DD Form 254 and attachments will be as prescribed by the procuring contracting agency concerned. In those instances in which the ACO, the quality assurance representative and the cognizant security office are a part of the same DCASR, separate copies shall be furnished to each so that they may discharge their individual responsibilities.

→ c. For Sub-subcontracts:

- (1) Prime contractor.
- (2) Appropriate ACO.
- (3) Subcontractor.
- (4) Sub-subcontractor.
- (5) Cognizant security office sub-subcontractor only.
- (6) Quality assurance representative.
- (7) Official identified in Item 12b, DD Form 254.
- (8) Others as necessary.

d. For solicitations (IFB, RFQ, RFP): Distribution of DD Form 254 for IFB, RFQ, or RFP, will be the same as for the prime contract, subcontract or sub-subcontract to which the solicitation is related, except that none is to be sent to the quality assurance representative.

62. Notification of Selection

The prime contractor shall immediately furnish in writing to the contracting officer or his designated representative, the names and addresses of each of the subcontractors to be engaged on classified work under a prime contract and the highest classification of information that shall be released or developed thereunder.

63. Unsatisfactory Security Conditions

If notified by a cognizant security office of unsatisfactory security conditions within a subcontractor's facility, contractors shall follow the instructions they receive from the contracting officer relative to what action, if any, should be taken in order to safeguard classified material relating to their subcontract.

64. Disposition of Classified Information ←

The subcontractor shall destroy classified material as provided by paragraph 19 unless the prime contractor requests return or authorizes retention. However, the prime contractor shall obtain the approval of the contracting officer or his designated representative authorizing a subcontractor to retain classified information. ←

65. Subcontracting With Foreign Industry

The U.S. has Industrial Security Agreements with Canada, the U.K., Australia, Sweden, Switzerland, the Netherlands, and the Federal Republic of Germany. Under the agreements with these nations, subcontracts involving U.S. classified information may be placed with industry in these countries. The security of the subcontracts will be governed by the appropriate regulations of the foreign governments concerned. However, before classified information may be released to a firm in one of these countries, approval must be obtained from the contracting officer. In addition, special security requirements clauses shall be incorporated in all subcontracts awarded to firms in these countries. Copies of these clauses may be obtained from the contracting officer.

66. Subcontracts Arising From Foreign Classified Contracts

A U.S. contractor awarded a foreign classified contract by a government with which the DoD has entered into a bilateral industrial security agreement may, unless specifically prohibited therein, subcontract within the U.S. in accordance with the provisions of this Manual; within the country of the contracting foreign government in accordance with instructions furnished by the designated agency of that government through the EDIS, HQ DLA; and within any other country only with the permission

of, and under conditions agreed to by, the contracting government, and the government of the country of the subcontractor, which shall be furnished to the contractor through the EDIS, HQ DLA. In those cases where U.S. classified information is involved in the

subcontract, the contractor or foreign government, shall, prior to its release to the foreign government, obtain an export letter/license authorization from the Department of State or specific approval of the U.S. User Agency which originated the information.

SECTION VII CONSULTANTS

67. General

a. Facility security clearance requirements for consultants to User Agency activities and contractors shall be determined in accordance with this Section.

b. In all cases, consultants shall have valid personnel security clearances issued in accordance with the requirements of this Manual.

- (1) If a consultant is cleared as a facility, he assumes complete responsibility for safeguarding of classified information in accordance with the provisions of this Manual.
- (2) If a consultant is not cleared as a facility and is performing under the provisions of paragraph 68, for purposes of briefing, debriefing, visiting, and reporting under provisions of this Manual, the consultant shall be considered to be an employee of the using contractor or User Agency activity. For consultants performing under the provisions of paragraph 70, the consultant's regular or full-time employer shall perform these duties on behalf of the contractor or User Agency activity for whom the employee is acting as a consultant.

c. The clearance status and safeguarding ability of a Type C consultant's regular employer shall be obtained from the employer's cognizant security office prior to the disclosure or release of any classified information to the consultant.

68. Consultant—Type A

The consultant does not possess classified material except at the using contractor's

cleared facility, on the premises of a User Agency activity or while on visits authorized under Section V.

a. The requirement for a separate facility security clearance for the consultant (including the execution of the DD Form 441 and the DD Form 441s by the consultant), or to have an existing facility security clearance raised, shall be waived provided the using contractor or User Agency activity, the consultant (and the chief executive of the consulting firm, if they are not one and the same), and all the consultant's employees who shall have access to classified information (such as employees shall be designated by name), jointly execute a certificate as follows:

- (1) Except in connection with authorized visits, classified material shall not be possessed by the consultant off the premises of the using contractor or User Agency; the using contractor or User Agency shall not furnish classified material to the consultant at any other location than the premises of the using contractor or User Agency, and performance of the consulting services by the consultant shall be accomplished at the activity of the using contractor or User Agency; and classification guidance will be provided by the using contractor or User Agency.
- (2) The consultant and his certifying employees shall not disclose classified information to unauthorized persons.
- (3) The using contractor or User Agency shall brief the consultant as to the security controls and procedures applicable to the consultant's performance.

DoD 5220.22-M

b. One copy of such certificate shall be furnished by the using contractor to his cognizant security office. In the case of a consultant to a User Agency activity, the certificate shall be retained by the Commander or Head of that activity.

c. The consultant (and the chief executive of the consulting firm, if they are not one and the same), and all certifying employees, shall complete the forms required by paragraph 26. These forms shall be submitted to DISCO through the User Agency activity or the contractor for which the consulting service is to be performed. Each application for clearance shall be accomplished by a copy of the certificate prescribed by paragraph a, above. The Letter of Consent shall be issued to the using contractor or User Agency activity, as appropriate.

d. Failure to accomplish the certification described above shall require the processing of a facility security clearance as prescribed by paragraph 21.

69. Consultant—Type B

The consultant possesses classified material at his place of business or residence, the consultant having full responsibility for security of the classified material.

a. A facility security clearance is required for the consultant to cover the premises at which he will possess the classified material and perform the consulting services.

b. Consultants of this type shall be considered to be prime contractors to the User Agency activity or subcontractors to the using contractor.

c. The provisions of this Manual pertaining to contractors or subcontractors, as appropriate, shall apply.

70. Consultant—Type C

The consultant possesses classified material at his regular employer's cleared facility, the consultant and his employer having agreed as to their respective responsibilities for security of the classified material.

a. No requirement exists for a separate facility security clearance for the consultant (including execution of the DD Form 441 and the DD Form 441s for the consultant), or to have an existing facility security clearance raised, provided the employing facility and the employee who is acting as a consultant to another contractor or to a User Agency activity are both cleared for access to at least the category of classified information as that to which the consultant will require access, and provided the employing facility and the employee jointly execute a Letter Agreement to Safeguard Classified Information for an Employee Performing Consultant Services (see Appendix I, paragraph W) by which the employing facility and the employee agree:

- (1) To place classified material which the consultant-employee must have in his possession into the employing facility's accountability system.
- (2) To incorporate procedures in the employing facility's SPP which prohibit the dissemination of the classified material within the facility, except that appropriately cleared personnel of the facility may be designated in writing on a strict need-to-know basis to provide the consulting employee clerical, destruction, and reproduction services necessary to his performance as a consultant.
- (3) To furnish the employee who is acting as a consultant a storage container so that the classified material may be stored under his control. Access to the storage container shall be limited to the employee who is acting

as a consultant and the minimum number of employees designated in accordance with paragraph (2) above, which are essential to support the consultant.

- (4) To advise its cognizant security office immediately upon any change in the consultant's status as an employee of the facility.

b. One copy of the Letter Agreement described in paragraph a., above, shall be furnished by the employing facility to its cognizant security office, and one copy to the contractor or User Agency employing the consultant.

c. In the event it is necessary to raise the consultant's personnel security clearance to a higher level (not above that of the employing facility), the consultant shall complete the forms required by paragraph 26 and submit them through the employing facility to

DISCO with a copy of the Letter Agreement prescribed in paragraph a., above. (If required to be cleared to a higher level than that of the employing facility, the consultant shall be processed for a separate facility security clearance in accordance with paragraph 67 and be required to maintain a security program fully independent of that of his employer.)

71. Consultants to User Agencies Employed Under Civil Service Procedures

Security clearances for persons employed as consultants to User Agencies under Civil Service procedures normally will be issued under the separate regulations of the User Agency concerned. However, User Agencies may process such a consultant for a personnel and/or facility clearance under the provisions of paragraphs 68-70 when deemed desirable.

SECTION VIII

PARENT-SUBSIDIARY AND MULTIPLE FACILITY ORGANIZATIONS

72. Parent-Subsidiary Relationship

a. When a parent-subsidiary relationship exists between two companies, the parent company must have a facility security clearance of the same or higher classification level as the subsidiary company, unless by formal action of its board of directors or similar executive body (i) it is excluded from access to all classified information held by the subsidiary company or (ii) it is excluded from access to classified information held by the subsidiary company which is of a higher classification level than the parent company's facility security clearance. However, if the parent company is foreign owned, controlled, or influenced, exclusion action may not be taken. In such circumstances, the subsidiary company is ineligible for a facility security clearance. (Certain exceptions to this rule can be made when the foreign ownership or control is exercised by a Canadian or U.K. interest. Consult the cognizant security office for details.) Each exclusion action shall be made a matter of record in the minutes of the executive body of both the parent company and the subsidiary company. Two copies of both sets of minutes shall be furnished to the cognizant security office of each cleared subsidiary company, along with a copy of the DD Form 441s, executed independently by the excluded parent company and the subsidiary company. In addition, when officers or directors of a subsidiary hold similar positions with the excluded parent company, they shall execute one of the following certificates, as appropriate; (i) I understand that the (name of parent company) is not cleared for access to classified information and I certify that I shall not disclose classified information to the (name of parent company)

or any of its agents regardless of my official business or personal association therewith, or (ii) I understand that (appropriate classification level) is the highest level of classified information which may be disclosed to the (name of parent company) or any of its agents regardless of my official business or personal association therewith. Official notice of the execution of each such certificate shall be made a matter of record in the minutes of the executive body of the subsidiary company and two copies of the minutes shall be furnished to the cognizant security office of the subsidiary. Two copies of each certificate executed in accordance with the requirements of this paragraph shall be furnished to the cognizant security office of the subsidiary.

b. Interchange of classified information and visits between a parent and its subsidiaries or between the subsidiaries shall be accomplished in the same manner as an interchange between a prime contractor and a subcontractor. However, in the case of a classified contract awarded to a subsidiary, the subsidiary, as necessary in the performance of the contract, may release classified information to the parent when required provided the parent company has an appropriate facility security clearance and safeguarding ability. Moreover, where the parent organization is owned or controlled by a foreign interest the U.S. subsidiary shall not release U.S. classified information to the parent except with the express written authority of the contracting User Agency. In such cases visits between the subsidiary and the parent shall be considered as Category 1 visits as defined in paragraph 41a. Neither the subsidiary nor the parent may release or disclose classified information pertaining to

the contract of the subsidiary to other subsidiaries of the parent without specific approval of the contracting officer or his designated representative or unless within the provisions for exception set forth in paragraph 5x.

c. In the case of two or more collocated cleared facilities (occupying the same office space or located side by side) consisting of a parent corporation and one or more wholly owned subsidiaries (100% stock ownership), the parent may request cognizant security office approval of a formal written agreement between the parent corporation and the subsidiary(ies) to utilize common security services for: (i) personnel security administration, (ii) document control (to include storage), (iii) reproduction, (iv) visitor control and, (v) other similar administrative services. In all cases the agreement shall be incorporated into the SPP (or appropriate supplement to an SPP) applicable to the facilities involved. The proposed SPP shall be submitted to the cognizant security office as part of the request. The SPP shall establish workable security procedures and clearly fix responsibility for security administration within the collocated facilities. The procedures shall be structured (e.g., separate accountability systems) to ensure that the need-to-know principles outlined in the previous paragraph are not violated. One facility security supervisor shall be designated for all facilities; the designee shall be considered an OODEP of these facilities and shall require a concurrent clearance at each facility. Appropriately authorized (cleared with a need-to-know) personnel rendering security services shall be designated in the agreement by job title to provide the specific services agreed to. Additionally, procedures may be incorporated into the SPP whereby a machine run or other roster (e.g., record of clearance) may be used in lieu of a visit letter provided such records are maintained in a current status at all times. When combined, the SPP and the roster shall provide the essential information required in paragraph 37d.

73. Multiple Facility Organizations

In the case of a multiple facility organization the contractor (HOF) is responsible for insuring the adherence, by each of its cleared operating locations, to the terms of the DD Form 441 and the security requirements of each classified contract being performed. A copy of the basic Security Agreement, with Appendage, shall be furnished to each facility listed in the Appendage and to each cognizant security office concerned. The HOF shall have a facility security clearance of the same or higher level as any cleared facility within the organization. Classified information may be interchanged among the cleared facilities of a multiple facility organization when the contractor determines that such interchange is essential to the fulfillment of a contract. Before the contractor places classified information or work in a facility of his organization, it shall have been determined that it has an appropriate facility security clearance and the capability to safeguard the classified material. The contractor shall provide the facility performing the work and its cognizant security office with classification specifications extracted from the DD Form 254 or other appropriate classification guidance. Revised guidance or notice of the reaffirmation of existing guidance, as applicable, shall also be provided. The SPP of a contractor having two or more facilities shall include security instructions which provide the controls necessary to protect classified information within the organization. These, among other procedures shall include, but not be limited to, instructions for the transmission of classified information and for visits of his employees between his cleared facilities. Such visits shall be considered as Category 1 visits as defined in paragraph 41a. Within each facility the SPP shall be adapted, as necessary, to meet local conditions, as prescribed by paragraph 5s. If the contractor elects to have Letters of Consent issued to (i) the HOF or (ii) one or more PMFs of the multiple facility organization, the SPP shall identify each subordinate facility (both cleared and un-

→ cleared) within their respective area of cognizance wherein a cleared individual(s) is employed or physically located. When a PMF(s) is established the HOF SPP will specifically reflect that all associated security responsibilities have been delegated to the PMF(s) for its specifically defined geographical or functional area. In all cases where the aforementioned cleared individuals are employed by or physically located at uncleared facilities falling under the cognizance of the respective HOF or PMF(s), the SPP shall reflect that the HOF or PMF, as appropriate, is responsible for personnel security administration. Such responsibilities will include meeting security education and paragraph 6 reporting requirements for all cleared personnel located/employed at these uncleared locations. In order to assure the security awareness of these cleared personnel, at their respective U.S. uncleared facilities falling within the set DCASR boundaries, (see Appendix VIII) the respective HOF or PMF security supervisor, or his appropriately cleared representative, shall visit each of these locations on an annual basis. Regarding the briefing of cleared personnel employed or physically located outside of the DCASR boundaries, such briefings will be handled as required in paragraph 97. Other considerations applicable to visits to

→ uncleared facilities are as follows:

→ a. As an alternative to annual visits to the aforementioned uncleared U.S. locations the HOF or PMF(s) may develop procedures which provide (i) equal or better assurance than annual visits, (ii) that all aspects of personnel security administration will be properly accomplished, (iii) that proper management attention is directed on a continuing basis to this area, and (iv) that responsibility and authority for accomplishment is formally assigned to cleared managerial personnel. Such procedures will be clearly set forth in the HOF or PMF(s), as appropriate, SPP and shall require the approval of their cognizant security office prior to being placed into effect.

b. Records which reflect the accomplishment of these requirements will be maintained as provided for in paragraph 26k.

74. Temporary Help Suppliers

a. *General.* A temporary help supplier is a subcontractor who dispatches personnel on his payroll to perform work on the premises of the using contractor or User Agency (see paragraph 5ab). A temporary help supplier and his field, branch or associate offices having a valid parent-subsidiary or multiple facility relationship are covered in paragraphs 72 and 73 respectively. The following paragraphs are concerned with:

- (1) A temporary help supply licensor (hereinafter referred to as the licensor) who grants licenses or franchises to other individuals or firms to use the name, administrative support, methods of operation or style of the licensor in a specific geographic area; or
- (2) A license or franchise holder (hereinafter referred to as a licensee) that is owned and operated by a legal entity separate and distinct from the licensor, and is licensed or franchised to do business under the name, method of operation or style of the licensor.

b. Where the temporary help personnel are actually employees of, and on the payroll of the licensee, the licensee may be granted a facility security clearance as provided for in this Manual.

c. Where the temporary help personnel are employees of, and on the payroll of the licensor, normally there would be no valid basis for the licensee to be granted a facility security clearance. As an alternative, a facility security clearance may be granted in the name of the licensor at the address of the licensee if there is a valid requirement for employees of the licensor to have access to

classified information at a contractor facility or User Agency activity, provided that:

- (1) The licensor has a facility security clearance at its home office; and
- (2) An employee of the licensor located on the premises of the licensee is appointed as security supervisor for the licensor; or
- (3) An employer-employee relationship is established between the licensor and at least one or more employees of the licensee through execution of a separate written agreement between the parties or by insertion of a clause in the franchise or license agreement. The agreement or clause shall specifically provide that, for a consideration, one or more employees of the licensee will act as security supervisor for the licensor in the territory covered by the license or franchise. One signed copy or certified true copy of the agreement or clause shall be furnished by the licensor to the cognizant security office concerned.

d. If the provisions of paragraphs c(1) and (2) or c(1) and (3) above, are followed, a facility security clearance may be granted to the licensor at the address of the licen-

see. This location will, for industrial security purposes, be considered as an operating facility of a multiple facility organization. Among other things, the SPP of the operating facility shall specify the functions and responsibilities of the security supervisor and the procedures for:

- (1) Processing personnel security clearances, including the granting of company CONFIDENTIAL clearances by the security supervisor.
- (2) Accomplishing the requirements of paragraphs 5 and 6 which relate to its (temporary help) personnel.
- (3) Processing visit requests dispatching its temporary help personnel to the using contractor's facility as Category 1 visits (see paragraphs 5ab and 41a).

e. When a licensee has a license or franchise agreement with more than one licensor, a facility security clearance may be issued in the name of each licensor. Similarly, if a contractor is engaged in a business which requires a facility security clearance in connection with such business and, in addition, is a licensee for a temporary help supplier, a facility security clearance may be issued in his own firm's name and one in the name of the licensor.

SECTION IX

SENSITIVE COMPARTMENTED INFORMATION AND COMSEC INFORMATION

→ 75. Sensitive Compartmented Information

a. The provisions of this Manual apply to research, development, and production of SENSITIVE COMPARTMENTED INFORMATION. In addition, special security requirements supplementing this Manual will be prescribed by the contracting department for SENSITIVE COMPARTMENTED INFORMATION contracts, except that for SENSITIVE COMPARTMENTED INFORMATION contracts awarded by military department procurement activities for the NSA, the NSA will prescribe the special security requirements.

→ *b.* In the case of SENSITIVE COMPARTMENTED INFORMATION contracts awarded by military department procurement activities for the NSA, the NSA shall be responsible for exercising security controls over the contract.

→ *c.* In the case of SENSITIVE COMPART-

MENTED INFORMATION contracts awarded by and for a military department or DoD Agency, an activity designated by the contracting military department or DoD Agency shall be responsible for exercising security controls over the contract. ←

d. Access to SENSITIVE COMPARTMENTED INFORMATION will be granted to contractor employees requiring access by the activity designated to exercise security controls over the contract as provided above. ←

e. Denial or revocation of authorization for access to SENSITIVE COMPARTMENTED INFORMATION is not appealable. ←

76. COMSEC Information

The contractor shall protect classified COMSEC information in accordance with the requirements of the COMSEC Supplement to this Manual.

SECTION X GRAPHIC ARTS

77. Special Requirements for Graphic Arts

This Section of the Manual provides specific security measures for the safeguarding of classified information during the development stages, performance of service, or production of material by the graphic arts industry. The security measures apply whether the work is performed by the prime contractor on his premises or subcontracted to a graphic arts facility.

78. Production Control Records

While the production control records remain with the classified job to which they relate, they shall be (i) plainly and conspicuously marked or stamped (not typed) at the top and bottom with the same classification as the material being produced, or (ii) unless the production control record itself contains classified information, covered over with a cover sheet conspicuously marked or stamped (not typed) at the top and bottom with the same classification as the material being produced. In either case, the additional markings required by paragraph 11b shall be applied as appropriate. Such production control records or cover sheets, unless they contain or have permanently attached thereto classified information, shall be marked with a notation indicating that they are unclassified when separated from the classified material being produced. The contractor may, at his discretion, use the production control records as the records required by paragraphs 12 and 18, provided they contain the required information and are retained for the period of time specified in paragraph 12.

79. Area Controls—Additional Requirements

During the layout, composition, platemaking, presswork and bindery stages of the production of classified material, controls shall be established to deny unauthorized personnel access to the immediate area in which such work is being performed. In the event the safeguarding requirements prescribed in paragraph 16 are insufficient for this purpose, such areas shall be designated as Restricted Areas and shall be controlled in accordance with the provisions of paragraph 34b. Additional requirements are:

a. Pressrooms. While the press is being made ready or being run, the press itself shall be identified and marked the same as the classified information being run. The press shall remain so identified until the run has been completed and all classified material removed. Marking and identification of the press is not required for press runs of short duration provided the run is completed prior to the end of the working day. Plates, blankets, chases, etc., need not be removed from the press at close of working hours, when the press run is incomplete, provided the area meets the requirements of paragraph 34a(3).

b. Composition Areas. Linecasting (e.g., intertype, linotype) and photocomposition machines shall be identified and marked the same as the classified information being set in type, except for jobs of short duration completed prior to the end of the working day. Slugs (i.e., lines cast on a linecasting machine), coded tapes, ribbons, negatives, etc., need not be removed from the machines

at the close of the working day when the composition is not completed, provided the area meets the requirements of paragraph 34a(3).

c. Bindery Area. Bindery areas shall be secured by the same method as pressroom areas.

d. Darkrooms. Admittance to all film processing units shall be restricted to cleared personnel who are assigned to the particular job or jobs involving classified information.

e. Proofreading Areas. Proofreading areas shall be controlled by physical barriers capable of preventing visual or audio access and entrance by unauthorized persons.

f. Shipping Entrances. Shipping entrances shall be secured when classified information is in the area. Loading and unloading operations shall be performed under the supervision of a cleared employee of the contractor.

80. Special Conditions

a. Overruns. All assembled copies of printed material not spoiled during a printing operation, which are in excess of the number of copies ordered, shall be designated as overruns. Overruns shall be held to a minimum. An exact count of the overruns shall be maintained and they shall be accounted for as prescribed in paragraph 12. Overruns shall be transmitted to the customer with the balance of the job or promptly destroyed in compliance with the provisions of paragraphs 19a through e.¹

b. Proofs. A record shall be kept of the number and disposition of proofs. Galley or page proofs approved by the customer shall be retained until the product is delivered and shall then be returned to the customer along with the original manuscripts.¹

¹ Where the classified production has been accomplished on the premises of the contractor, as opposed to being done by a graphic arts subcontractor, the disposition of overruns, proofs, samples and other material, except for waste, used in the production of the job may be delayed until the completion or termination of the contract concerned.

c. Waste Disposal. The contractor shall provide properly identified waste containers at each production point at which waste, spoilage, trimmings, or cuttings accumulate. Waste shall include paper stock used for press makeready, spoilage during running, printed copies spoiled during bindery makeready, or excess copies of individual pages which are not to be assembled to form a complete product. Waste containers shall be adequately safeguarded and the waste promptly destroyed in accordance with paragraph 19f. Waste shall not be retained in production areas during nonworking hours.

d. Return of Samples. All graphic arts samples (i.e., classified material furnished by the customer for reproduction) shall be returned to the customer immediately after the completion of the work.¹

e. Bulk Shipment. Graphic arts products that are shipped in bulk in double containers will be stacked in the inner container face up. A cover sheet shall be placed on top of the material before sealing the inner container. The contractor shall maintain a record of the quantity shipped in each container, and when copies are serially numbered, the contractor shall number the inner containers, and the record shall show which serial numbers were packed in each container. Such records shall be incorporated into the control station records maintained in accordance with paragraph 12. The classification markings, and if appropriate, the notations prescribed in paragraph 11b, shall be stamped on all outside surfaces of the inner container. Outer containers shall be sealed by wire stapling or by tape so that tampering will be evident. No markings shall be made on the outer containers which will in any way indicate that the package contains classified material. Address labels will be placed on the top surface of both containers, and receipts will be placed inside the inner container.

f. Materials Used in Production.

- (1) All materials used in production which contain classified informa-

tion, (i.e., negative flats, layouts, masters, dummies, vellums, stencils, composition tapes, proofs, tympan sheets, negatives, type, plates, etc.) shall be safeguarded in accordance with paragraphs 14 and 16 and immediately after completion of the work shall be destroyed in accordance with paragraph 81 or returned to the customer along with the job on which they were used¹ (see paragraph 12f for accountability requirements).

- (2) Plates and rubber blankets, after use on a classified production, may be re-used only on classified production, provided they are stored between runs as specified in paragraph 14. The plates and rubber blankets shall be identified as provided in paragraph 11a(8), and the classification marking shall at all times reflect the highest category of classified information for which the plate or rubber blanket has been used (see paragraph 12f for accountability requirements). Plates and rubber blankets used for classified productions, when no longer serviceable, or re-use is not desired, shall be destroyed as prescribed in paragraph 81. A contractor is not authorized to turn over classified plates to a subcontractor for the sole purpose of regaining such plates. Moreover, the regaining of plates shall not be considered as an authorized method of destruction under paragraph 81.
- (3) Blankets, other than rubber, used on classified productions, shall not be re-used and shall be destroyed as prescribed in paragraph 81.
- (4) "Rollers" and other parts of

presses which retain impressions of classified information during the printing stages shall be cleaned to remove the classified information upon completion of the run.

81. Destruction—Special Requirements

Classified material used in the reproduction process shall be destroyed in accordance with paragraph 19c, except that:

- a. Classified information on metal foundry and wooden type shall be considered as having been destroyed when the type is redistributed in the type case.
- b. Classified information on glass negatives shall be destroyed by dissolving the emulsion or by pulverizing.

82. Mailing Lists

a. *Classified*. When a mailing list, used for the distribution of unclassified material, is classified, the material shall be protected as though classified (markings not required) until separated from the classified mailing list during the production process or at the point of mailing or shipping.

b. *Unclassified*. When a mailing list, used for the distribution of classified material, is unclassified, the list shall be protected as though classified (markings not required) until separated from the classified material during the production process or at the point of mailing or shipping.

c. *Related Material*. When classified mailing lists are prepared or maintained by a contractor, all material which retains an impression of the addresses, such as carbons, addressing plates, identification strips, and verification lists shall be classified and safeguarded accordingly.

SECTION XI

NATO INFORMATION

83. Application

This Section of the Manual provides for the additional security measures which have been established for the safeguarding of NATO classified information. The provisions contained in this Section supplement the provisions of Sections I through X of this Manual. These additional security measures apply whether the NATO classified information is in the possession of the prime contractor or in the possession of his subcontractor(s).

84. Authority

The requirements of this Section reflect the security procedures established by the U.S. Security Authority for NATO affairs for the safeguarding of NATO classified information in the possession of U.S. industry.

85. Supervision and Orientation Requirements

a. The contractor who receives NATO classified information shall appoint a responsible officer (one who is required to be cleared as part of the facility security clearance) to supervise and direct the security measures in relation to NATO classified information.

b. The contractor shall maintain a separate record of all employees located at the facility who have been authorized access to NATO classified information, in addition to the clearance record required by paragraph 28.

c. The contractor shall notify all of his personnel who will have access to NATO classified information that:

- (1) The term "NATO classified information" used in this Section applies to classified information circulated within and by NATO, including information received from member nations as well as information originated in the organization itself. However, classified information contributed by a member nation remains the property of the originating nation even though it is circulated in a document belonging to NATO.
- (2) The marking "NATO" on a document is used to signify that the document is the property of NATO. The marking "COSMIC" is also used on a NATO (TOP SECRET) document to signify that it is the property of NATO and that it is subject to special security controls.
- (3) COSMIC TOP SECRET documents, NATO SECRET documents and NATO CONFIDENTIAL documents shall be protected according to the rules in other Sections for TOP SECRET, SECRET, and CONFIDENTIAL material and the additional rules prescribed in this Section. NATO documents marked "RESTRICTED" which are furnished to the contractor shall be marked and protected as prescribed in paragraph 11d.
- d. The contractor shall bring to the attention of all of his personnel who will be authorized access to NATO classified information their continuing individual responsibilities for safeguarding NATO classified information; further, they shall be advised that when they are in other NATO countries

they may be subject to the laws of those countries which pertain to the handling of classified information. When access to COSMIC TOP SECRET information is involved, the employee shall sign a certificate to the effect that he has been briefed on his responsibilities for safeguarding COSMIC TOP SECRET information.

86. Security Clearances

a. A final personnel security clearance granted by DISCO for a U.S. citizen is valid for access to NATO information of the same or lesser security classification provided the individual has been given a security briefing in accordance with paragraph 85*d* above. Immigrant aliens or aliens issued U.K. or Canadian Reciprocal clearances are not authorized access to NATO classified information (see paragraphs 20*c*, 24*a*(2) and 31*d*).

b. All contractor employees who require access to NATO information classified CONFIDENTIAL shall be cleared by DISCO (see paragraph 24*a*(1)(*c*)).

c. Application for a security clearance for employees requiring access to NATO CONFIDENTIAL information shall be made by the contractor as provided for in paragraphs 24, 26 and 27 for U.S. citizens.

d. An interim CONFIDENTIAL or interim SECRET clearance granted by DISCO is not valid for access to NATO information classified CONFIDENTIAL or SECRET.

e. Contractor employees who require access to NATO RESTRICTED information shall be cleared by the contractor in accordance with paragraph 24*b*.

87. Reproduction, Preparation, and Marking

a. Requirements in paragraph 18 and Sec-

tion X apply equally to the reproduction of NATO classified documents. However, except for COSMIC TOP SECRET information, no special permission is needed to include references to, extracts from, or paraphrases of NATO classified documents in other documents which the contractor must prepare in the performance of the contract. In the case of COSMIC TOP SECRET information, reproduction requests shall be forwarded to the Central U.S. Registry for authorization. Address: Central U.S. Registry, Washington, D.C. 20310.

b. Requirements in paragraph 11 apply equally to the marking of NATO classified documents. A SECRET, CONFIDENTIAL, or RESTRICTED document which is reproduced from a NATO document shall be marked NATO at the top and bottom, in addition to the classification markings, and a TOP SECRET document which is reproduced from a NATO document shall be marked COSMIC at the top and bottom in addition to the TOP SECRET marking.

88. Transmission of NATO Material

a. When NATO SECRET or CONFIDENTIAL material is prepared for transmission and an inner container is required by paragraph 17*a*, that container shall be marked NATO in addition to the classification marking. When transmitting NATO TOP SECRET material the inner container shall be marked COSMIC in addition to TOP SECRET.

b. The transmission of NATO classified information within the U.S. shall be in accordance with the procedures set forth in paragraphs 17*b*, *c*., and *d*. except that the minimum requirement for mailing NATO CONFIDENTIAL information is U.S. Registered Mail.

c. All NATO classified information furnished to a U.S. contractor in connection

with a U.S. classified contract shall be transmitted to destinations outside the U.S. only with authority of the contracting officer. If such information is to be returned to the U.S., approval of the contracting officer is not required.

- (1) COSMIC TOP SECRET going from or being sent to the U.S. shall be transmitted to the Chief, Central U.S. Registry, The Pentagon, Washington, D.C. 20310 by one of the methods authorized by paragraph 17b for forwarding to the intended destination.
- (2) NATO SECRET and NATO CONFIDENTIAL information going from or being sent to the U.S. shall be transmitted by the contractor via one of the means authorized in paragraph 17e. Information going to a NATO activity outside the U.S. shall be transmitted to an appropriate U.S. activity for forwarding to the NATO activity. NATO classified information coming to the U.S. shall be transmitted through an appropriate U.S. Government activity to the U.S. contractor.

d. NATO classified information furnished to a U.S. contractor in connection with a NATO, or NATO member country, classified contract or project shall be transmitted to destinations outside the continental limits of the U.S. only with the authority of the contracting officer. If such information is returned to the U.S., approval of the contracting officer is not required.

- (1) COSMIC TOP SECRET shall be transmitted as prescribed in paragraph c(1) above.
- (2) NATO SECRET and NATO CONFIDENTIAL information shall be transmitted as prescribed in paragraph c(2) above.

e. All NATO classified bulky material, of any category, shall be sent through channels established by the cognizant security office on instructions from the EDIS, HQ DLA.

89. Functions of the Contracting Officer

a. When a U.S. contractor enters into pre-contract negotiations involving NATO classified information with a U.S. contracting officer, the contractor shall obtain his instructions from the contracting officer concerned as prescribed in this Manual.

b. When a U.S. contractor enters into pre-contract negotiations with a NATO government other than the U.S., a contractor of such NATO country, or a NATO international body requiring that the contractor have possession and access to NATO classified information in the U.S., the U.S. contractor shall request necessary instruction from the contracting officer of such NATO country or international body.

90. NATO Reporting Requirements

The contractor shall immediately report through the cognizant security office to the Chief, Central U.S. Registry, The Pentagon, Washington, D.C. 20310, receipt of COSMIC TOP SECRET information from a source outside the U.S. when the information has not been transmitted via the Central U.S. Registry. A copy of the report shall be sent to the EDIS, HQ DLA. The contractor shall report to the cognizant security office receipt of NATO SECRET or CONFIDENTIAL information from any source other than through a U.S. Government activity unless the information is received in connection with approved visits (e.g., attendance at a bidders' conference).

91. Subcontracting

Prior to negotiating a NATO classified

subcontract in the U.S. or in another NATO country, a U.S. prime contractor shall obtain permission to negotiate such a subcon-

tract from the contracting officer who let the prime contract or his designated representative.

SECTION XII OVERSEAS OPERATIONS

Part 1. ACCESS TO U.S. CLASSIFIED INFORMATION

92. General

a. This Part sets forth access, safeguarding and notification requirements for cleared U.S. citizen employees of U.S. contractors assigned to duty stations outside the U.S. These requirements also apply to U.S. citizens who, in addition to being cleared as employees of cleared U.S. contractors, are also dual-status employees of foreign subsidiaries which are wholly owned and controlled by cleared U.S. facilities.

b. This Part does not apply to:

- (1) Uncleared employees of cleared U.S. contractors who are stationed outside the U.S.;
- (2) U.S. citizens who are representatives of any foreign interest or employees of foreign subsidiaries of cleared U.S. facilities but do not hold dual-status employment with the owning or controlling U.S. facility; and
- (3) Representatives (not employees) of cleared U.S. contractors.

c. Cleared employees of U.S. contractors stationed overseas are encouraged to attend periodically scheduled security briefings conducted by the OISE. These briefings are designed to familiarize the employees with the international aspects of the Defense Industrial Security Program and the security requirements unique to the foreign countries in which the contractor does business.

93. Access to Classified Information

Contractors are authorized to grant access to U.S. classified information to their cleared employees who are assigned overseas, subject to the following:

a. Access to U.S. classified information identified in this paragraph shall be granted only with the prior written approval of the User Agency having primary interest if the information concerned is:

- (1) TOP SECRET information.
- (2) RESTRICTED DATA or FORMERLY RESTRICTED DATA.
- (3) COMSEC and SENSITIVE COMPARTMENTED INFORMATION (see paragraph 6, CSISM).
- (4) Special Access Programs information (see paragraph 5*t*).
- (5) Information for which foreign dissemination has been prohibited in whole or in part.

b. Access shall be limited strictly to that information required by the employee for performance of the specific duties or contracts for which he is assigned overseas. Further, access to U.S. classified information under this Section shall be made, to the maximum extent practical, on an oral or visual basis. When physical access is to be granted to an employee, the appropriate safeguarding provisions set forth in paragraph 94, shall be strictly complied with.

c. Access to U.S. classified information for cleared employees assigned overseas may be granted both in the U.S. and overseas.

d. Access to U.S. classified information granted to a cleared employee of a cleared U.S. facility who is also an employee of a U.S. wholly owned and controlled foreign subsidiary of such facility is granted only in his capacity as an employee of the cleared U.S. facility. The contractor granting the access is responsible for assuring that his employee provides adequate safeguards for any classified information disclosed to such employee. In addition, the contractor shall take action, as appropriate, to insure that U.S. classified information entrusted to the employee is not further released or made available to other employees of the foreign subsidiary.

94. Safeguarding U.S. Classified Information

The following additional safeguards are prescribed in connection with U.S. contractor overseas operations:

a. *Security Classification Guidance.* The contractor shall provide security classification guidance to employees performing outside of the U.S. on a classified contract, project or mission. As a minimum, such guidance shall consist of the DD Form 254, when a classified contract is involved, and shall cover all classified information relating thereto.

b. *Transmission.* Transmission of classified material to a cleared contractor employee located outside the U.S. shall be strictly in accordance with paragraph 17e. The material shall be addressed to a U.S. military activity or other U.S. Government activity and shall be marked for the attention of the contractor or the employee for whom it is intended. The U.S. Government activity will notify the contractor or contractor employee of the receipt of the material. Classified material will be transmitted only through U.S. Government channels. Normally, transmission will be by Registered Mail through the U.S. Military

Postal Service or by the ARFCOS. However, the contracting officer may authorize any of the other approved methods of transmission described in paragraph 17e. If disclosure authorization is required and has been obtained, it should be cited in the transmission document with the effective dates and any other limitations. The contractor shall make prior arrangements for the storage of U.S. classified material with a U.S. military installation, the OISE, a military attache, a MAAG, an ODC, or a U.S. diplomatic or consular officer prior to transmitting U.S. classified material overseas.

c. Custody and Storage

(1) Personnel authorized access to U.S. classified material overseas will normally be permitted such access at a U.S. Government activity only. The storage of U.S. classified material overseas at any location other than a U.S. military installation or U.S. Government-controlled installation is prohibited.

(2) If in the performance of a contract, project, or mission, it is necessary for a contractor employee to physically require temporary custody of U.S. classified material, authorization for removal shall be obtained from the U.S. Government activity. When such custody is authorized, the employee is responsible for personal possession and surveillance of the material at all times. Immediately following the purpose for which the material was needed and the removal was authorized, but in all cases prior to the end of the work day, the material is to be returned to the U.S. Government activity for storage purposes. Movement of the material while in the employee's custody shall be governed by the provisions of paragraph 17h.

d. Disclosure

Except as provided for in paragraph 48,

contractor personnel are not authorized to disclose classified information to any foreign government, commercial activity or entity, or to an international pact organization or to its representatives. Cleared contractor personnel overseas may, however, disclose classified information:

- (1) To other cleared personnel within their company who have been granted a Letter of Consent at the required level and who have a need-to-know for access to the information concerned.
- (2) To any appropriately cleared military or civilian member of a U.S. User Agency who has a valid need-to-know.
- (3) Outside the contractor's organization within the U.S. only in accordance with this Manual, and outside the U.S. only in accordance with instructions from the contracting officer of the User Agency.

95. Overseas Assistance

a. The DoD has established the OISE to provide administrative assistance for industrial security purposes to U.S. industry in their marketing, liaison, and technical assistance activities in Europe and adjacent geographical areas. The OISE is a field extension of the EDIS, HQ DLA-N, and functions under its operational and administrative control. The OISE acts as the central file in Europe for information pertaining to security clearances and security assurances for U.S. citizen contractor employees located outside the U.S. Such information from the file is available for official use by agencies and activities of the U.S. Government, foreign governments and NATO.

b. The OISE assists U.S. industry by (i) arranging classified visits for U.S. contractor employees; (ii) providing storage for

classified material; (iii) providing mail channels for transmission of classified material between a contractor in the U.S. and an approved destination in Europe when specifically authorized by HQ DLA-N; (iv) providing security briefings and security certificates as appropriate; and (v) providing assistance on security matters, such as visits to military activities or contractors in Europe.

c. The civilian street address of OISE is Office of Industrial Security, Europe, U.S. Defense Logistics Agency, 13 Chaussee de Louvain, 1940 St. Stevens-Woluwe, Belgium; telephone 720-8259. The APO address is: OISE, APO New York 09667; U.S. Government cable address is: OISE, BRUSSELS, BELGIUM; other cables: OISE, American Embassy, Brussels, Belgium; TELEX address is: OISE, American Embassy, 21336, Brussels, Belgium.

96. Notification of Overseas Assignment

a. Whenever a contractor assigns a cleared employee to an overseas duty station the contractor shall furnish the following information to DISCO on DLA Form 562-R: full name, Social Security Number, date and place of birth, level of access to U.S. classified information required overseas, passport or ID number, name and address of his new duty station overseas and, notice that the briefing required by paragraph 97 has been accomplished.

b. Upon receipt of this information, DISCO will forward a copy of the employee's Letter of Consent to OISE when the employee is assigned to an overseas location within the geographical jurisdiction of OISE. Subsequently, the contractor is required to provide written notice to DISCO, and OISE when appropriate, of any permanent change of mailing address in the overseas duty station of its employees, the reassignment of an employee to the U.S. or other changes in status as reflected in paragraph 6b(2).

c. Residence or assignment of cleared immigrant aliens outside the U.S., Puerto Rico, Guam, or the Virgin Islands for a period of 90 consecutive days or more in any 12-month period negates the basis upon which the Letter of Consent was issued, and the Letter of Consent will be administratively terminated without prejudice by DISCO upon receipt of contractor notification as outlined in paragraph 6b(6).

97. Security Briefings and Certificates

a. Cleared employees who are to be assigned to duty stations outside the U.S. are to be briefed on the security aspects of their new positions. These briefings are the responsibility of the contractor. If access to NATO classified information is or may be involved, the briefing shall also cover NATO security requirements as described in Section XI.

b. Each cleared employee assigned overseas shall execute and have witnessed a certificate attesting that:

- (1) He has received a security briefing and understands his responsibilities.
- (2) He will safeguard classified information in accordance with prescribed security standards.
- (3) The classified information to which he has been granted access will be used only for the purpose for which released.
- (4) He understands and accepts the fact that his Letter of Consent may be suspended or revoked for violation of security regulations or improper use of classified information.
- (5) He understands that he may be sub-

ject to action under the espionage statutes of the U.S. with respect to the classified information to which access is granted.

- (6) He understands that upon termination of the purpose for which he has been granted access, his responsibilities for safeguarding the classified information continue unabated until the security classification is removed by appropriate Government authority. The executed and witnessed briefing certificate shall be retained by the contractor for the duration of the overseas assignment.

c. Subsequent to the initial security briefing, each individual shall be given an annual refresher briefing. A certificate similar to that described above shall be executed annually and maintained as long as the individual is assigned overseas. The certificate shall be modified as necessary to reflect any change in the nature and extent of the classified information to which the individual requires access, and the scope and nature of the threat to which the overseas activity may expose the individual.

d. Normally, refresher briefings should be accomplished on the temporary return of employees to the U.S. or by a security representative of the contractor stationed overseas or on visits overseas. When this is not practical, the briefing and execution of the certificate may be accomplished by OISE at the request of the contractor. Outside areas serviced by OISE, the contractor may obtain a written briefing statement by mail from the employee.

e. The contractor shall assure that a company SSP, or supplement thereto, is prepared to cover security procedures at the contractor's overseas locations.

Part 2. ACCESS TO CLASSIFIED INFORMATION OF FOREIGN GOVERNMENTS AND INTERNATIONAL PACT ORGANIZATIONS UNDER A SECURITY ASSURANCE

98. General

In its relations with friendly and allied foreign governments, the U.S. has entered into various treaties and agreements whereby each signatory government agrees to safeguard the classified information released to it by the other government. These range from simple bilateral agreements providing only that each government will safeguard, in accordance with mutually agreed procedures, the classified information released to it by the other government, and that the information will not be disclosed to a third country without the consent of the originating government to multilateral treaties establishing international organizations for concerted defense. Such treaties usually contain either a technical annex establishing the detailed procedures and standards for safeguarding classified information originated or disseminated by the organization, or provisions authorizing the organization to establish mutually agreeable regulations for safeguarding such information.

a. Access to classified information of a foreign government or international pact organization (e.g., NATO) is granted by the activity possessing the information and the scope of access is governed by the regulations of the activity possessing and disclosing the information. Hence, this Part prescribes no specific limitations on the access to classified information of foreign governments or international pact organizations which may be afforded an individual under a Security Assurance determination. The responsibility for release of the information rests with the foreign activity or international pact organization, or with the contractor if the information had previously been released to him directly by the foreign government, the prime contractor, or an international pact organization without going through Government channels.

b. A contractor, or contractor employee,

granted access to foreign or international pact organization classified information must take note of the limitations prescribed relative to the further dissemination of such information. For example, NATO classified information cannot be stored in non-NATO countries or released to nationals of non-NATO countries, nor can NATO classified subcontracts be let to contractors of non-NATO countries. Foreign countries normally have restrictions on the disclosure and dissemination of their classified information to nationals of a third country.

99. Security Assurance

This paragraph establishes the procedures to assist U.S. cleared contractors in meeting personnel security requirements imposed by friendly and allied foreign governments and international pact organizations with whom the U.S. has entered into either a bilateral or multilateral security agreement for access by U.S. citizens to foreign classified material which is under the control of the foreign government or organization.

a. The contractor may make application for a Security Assurance by submitting a written request containing the information required by paragraph (3), below. Upon application by the U.S. contractor, DISCO will issue a Security Assurance (DISCO Form 382) for currently cleared contractor employees. If the employee does not have a valid Letter of Consent, the contractor will submit the following to DISCO:

- (1) The forms prescribed in paragraph 26c,¹ or;

¹ Under Item 9 of DD Form 48 or 49 or Item 7 of DD Form 48-3, the applicant shall list both his overseas residence and permanent U.S. residence if one is maintained. In addition, under Item 12 of DD Form 48-3, the applicant shall list all previous overseas residences. Under Item 19 of DD Form 48 or DD Form 49, or Item 11 of DD Form 48-3, the applicant shall show the names and addresses of all firms or foreign government activities with which the applicant is associated, the relationships and duties in connection therewith and the nationality of the controlling interests of the firms involved.

(2) Two copies of DD Form 48-3¹ if there has been less than a 12-month lapse in a prior employment at which time the employee was granted a Letter of Consent; and,

(3) A written request containing the following information:

(a) The title of the position and summary of the duties of the individual for whom the request is made.

(b) The name and location of the overseas office or activity to which the individual is assigned or attached for duty.

(c) The employee's passport or ID card number, if available.

(d) A justification² for the request which identifies the activity or the subject matter of the proposed visit, sales activity, or contract which will require a Security Assurance.

(e) A statement providing the name and address of the foreign government activity or international pact organization requesting the U.S. Security Assurance and the level of access required. If access to U.S. originated, and appropriately marked, classified information will be granted to the employee by the foreign requestor, the contractor will execute and maintain one copy of the brief-

ing certificate prescribed by paragraph 97.

(4) In the case of persons who are employees of foreign subsidiaries, the application shall be sent through the parent organization or the PMF.

(5) Upon termination of employment or assignment overseas, the Security Assurance determination is void and the contractor shall immediately notify DISCO of the individual's changed status by means of DLA Form 562-R, and return the individual's Security Assurance determination to DISCO.

(6) Requests for reinstatement of a Security Assurance determination will be processed in the same manner as an original request.

(7) If an individual on whom a Security Assurance has been given is subsequently employed by a cleared contractor and requires a U.S. security clearance, the contractor may make application within 12 months for a security clearance for the individual under Section III by submission of a DD Form 48-3 (see paragraph 26e). If the time lapse is more than 12 months, the forms prescribed by paragraph 26c shall be submitted.

b. Normally, requests for Security Assurance determinations will be limited by the foreign government or international pact organization to CONFIDENTIAL, or SECRET access. In exceptional cases, requests for TOP SECRET Security Assurance received from a foreign government or international pact organization will signify that access to TOP SECRET information is necessary for the consummation of a specific contract, project, or activity. TOP SECRET Security Assurance determinations shall be limited to the specific contract, project, or activity for which granted.

² The need and justification may be stated in general terms. For example: in order to participate in the negotiation of contracts with foreign governments or international pact organizations it will be necessary for him to have access to classified information of those countries and organizations (identify countries and/or organizations); or as our overseas electronics engineer, it will be necessary for him to have access to foreign classified information in order to service equipment sold by our company to (identify country or countries concerned).

SECURITY REQUIREMENTS FOR ADP SYSTEMS

SECTION XIII

100. Application and Purpose

This Section:

a. Establishes security measures for protecting classified information stored, processed or used in, and classified information communicated by ADP systems in the custody and control of contractors including computer service organizations providing contractual ADP services to the DoD or its contractors. Security measures for User Agency ADP systems operated by contractors are the responsibility of the controlling User Agency.

b. Specifies conditions and prescribes security requirements under which ADP systems will be operated when handling classified material. Additional security requirements may be levied for processing information associated with Special Access Programs as defined in paragraph 3*bm* (e.g., COMMUNICATIONS ANALYSIS and COMSEC information in accordance with Section IX).

c. Provides for the application of administrative, physical and personnel security measures required to protect classified material processed or resident in ADP systems from inadvertent or deliberate compromise.

d. Requires the initial approval, in writing, of the cognizant security office prior to processing any classified information in an ADP system.

101. Definitions

a. ADP System Access. The ability and the means to approach, communicate with (input to or receive output from), or other-

wise make use of any material or component in an ADP system.

b. ADP System. An assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention. An ADP system as defined for purposes of this Manual is the totality of ADP equipment and includes:

- (1) General and special purpose computers (e.g., digital, analog, or hybrid computer equipment);
- (2) Commercially available components, those produced as a result of research and development, and the equivalent systems created from them, regardless of size, capacity, or price, which are utilized in the creation, collection, storage, processing, communication, display and dissemination of classified information;
- (3) Auxiliary or accessorial equipment such as data communications terminals, source data automation recording equipment (e.g., optical character recognition equipment, paper tape typewriters, magnetic tape cartridge typewriters, and other data acquisition devices), data output equipment (e.g., digital plotters and computer output microfilmers), etc., to be used in support of digital, analog, or hybrid computer equipment, either cable-connected or self-standing.
- (4) Electrical accounting machines used in conjunction with or inde-

DoD 5220.22-M

pendent of digital, analog, or hybrid computers; and

- (5) Computer equipment which supports or is integral to a weapons system.

c. ADP System Security. Includes all hardware/software functions, characteristics and features, operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities, and the management constraints, physical structures and devices; personnel and communication controls needed to provide an acceptable level of protection for classified material to be contained in the computer system.

d. Central Computer Facility. One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area even though they are connected to the central computer facility by approved communication links.

e. Complex. A facility, or any element thereof, which consists of one or more buildings or structures physically enclosed within a common perimeter barrier supplemented by protective measures which prevent unauthorized entry and control authorized entry.

f. Contained. "Contained" refers to a state-of-being within limits, as within system bounds, regardless of purpose or functions, and includes any state of storage, use or processing.

g. Dedicated Mode. An ADP system is operating in a dedicated mode when the central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specified users or groups of users having

the same security clearances and access approvals for the processing of a particular type(s) and category(ies) of classified material.

h. Disconnect. A remote terminal or peripheral device is considered to be disconnected when at the Central Computer Facility:

- (1) It is unplugged, or
- (2) The power to the channels or transmission lines is switched off, or
- (3) When software disconnect routines are employed. However, software disconnect routines shall be used only in the case of information classified no higher than SECRET and which does not have Special Access requirements. Software disconnect routines must be:
 - (a) Documented so as to clearly indicate detail logic processes employed.
 - (b) Approved initially in writing by the cognizant security office.
 - (c) Verified by the contractor via written certification at least once every 90 days to insure continued effectiveness.
 - (d) Reapproved by the cognizant security office after ADP system modifications.

i. Escort. Escorts are duly designated personnel who have appropriate clearances and access authorizations for the material contained in the systems, and are sufficiently knowledgeable to understand the security implications of, and to control the activities and access of the individual being escorted.

j. Multi-Level Security Mode. An operation under an operating system (supervisor

or executive program) which provides a capability permitting various levels and categories or compartments of material to be concurrently stored and processed in an ADP system. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accommodate the concurrent processing and storage of (i) two or more levels of classified data, or (ii) one or more levels of classified data with unclassified data depending upon constraints placed on the systems by the cognizant security office.

k. Operating System. An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs, and play a central role in assuring the security operation of a computer system. Operating systems may perform debugging, input/output, accounting, resource allocation, compilation, storage assignment tasks, and other system-related functions. (Synonymous with monitor, executive, control program and supervisor.)

l. Remote Terminal. A device for communicating with an automatic data processing system from a location that is time, space or electrically distant.

m. Resource-Sharing Computer System. A computer system which uses its resources, including input/output devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities, to enable one or more users to manipulate data and process coresident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as time-sharing, multi-programming, multi-accessing, multi-processing, or concurrent processing.

n. Software. A set of computer programs, procedures and documentation concerned with the operation of an ADP system.

o. Transmission. For the purposes of this Section, the term includes radio, microwave, laser or other methods of transmissions, as well as cable and wire transmission.

102. General

a. The procedures and methods to be employed in safeguarding classified information will depend upon the nature of the ADP system and the use to which it is put. Accordingly, it is the contractor's responsibility to safeguard all classified information contained in the ADP system and insure that approved security controls are in effect and working satisfactorily. The contractor shall prepare an SPP defining personnel responsibilities and detailed security control procedures to be followed in the processing of all classified data in each ADP system. This SPP shall encompass, as a minimum, all of the pertinent elements contained in this Section plus all hardware and software verification and certification procedures required to insure initial and continued safeguarding of classified information in the system.

b. The contractor shall appoint an ADP systems security supervisor for each facility and an ADP systems security custodian for each ADP system approved for the handling of classified material. The ADP systems security supervisor, where different from the facility security supervisor, shall be responsible to the facility security supervisor for implementation of procedures and practices prescribed for the safeguarding and control of his respective ADP system.

103. Personnel and Physical Controls

a. Personnel.

- (1) Those personnel who develop, test and maintain application software pro-

grams, or use software systems which are classified, or which will be used to access or develop classified material shall have a personnel security clearance and need-to-know for the highest and most restrictive category of classified material which they can access under system constraints.

- (2) Personnel operating the system and controlling access to its entry points to that system, or those who design, develop, install, modify, service or maintain the security features of the software in the operating system which controls user program access to the system (input/output, storage or use) shall have a security clearance for the highest and most restrictive category of material contained or processed in the system, and shall be indoctrinated in appropriate security procedures for the particular ADP system and facility before assuming their duties. Temporary or permanent modification of the operating system shall be tested by appropriately cleared and specifically designated personnel to assure that the security features are effective. Audit trail records of these transactions shall be maintained.
- (3) Unescorted entry to the Central Computer Facility or access to any of its ADP system components (hardware or software) shall be controlled and limited to personnel who are cleared for access to the highest classification and most restrictive category of classified material contained or processed in the ADP system, and where need-to-know has been ascertained by the responsible ADP system security supervisor. All persons involved in maintenance or repairs requiring access to any part or component of the ADP system (central or remote) which could affect or modify the secure operation of the system or

permit access to classified data, shall have a security clearance for the highest and most restrictive category of classified information contained in or processed by the system. Shall it become necessary for maintenance personnel not possessing such clearances to access the system, they shall be accompanied by an escort duly designated by an ADP security supervisor for that purpose.

- (4) Other persons whose access to the area is required on a one-time or infrequent basis, and who will not have access to classified material or to the system's hardware or software, may be admitted to the area when accompanied by an escort who will be responsible for the visitor's activities while in the area.

b. Physical.

- (1) Closed Areas in conformance with paragraph 34a, shall be established for the Central Computer Facility and for rooms housing remote terminals authorized to access or process classified data. To maintain the integrity of the system, the controls of the areas will be maintained even during those periods when there is no classified information in the system. An exception to the requirement for continuous Closed Area controls can be made for systems in which all operations take place within the Central Computer Facility and all remote terminals are disconnected provided the following conditions are met:

- (a) That Closed Area controls are in effect during periods when classified information is being processed, is on line or is otherwise available.
- (b) That all internal memory and circuitry used for the storage of

classified data is cleared and verified by a responsible individual designated in the SPP prior to removal of Closed Area controls. All data storage devices (drums, discs, tapes, etc.) must be stored in accordance with paragraph 14, or be declassified in accordance with paragraph 105. All documentation on which classified information is recorded, including carbons and printer ribbons, must be removed and properly stored or destroyed. A log must be maintained to record the date and time the above actions were taken, and by whom.

(c) That all other applicable provisions of this Manual apply.

- (2) Before the ADP system is placed in an unclassified mode (unapproved remotes reconnected and/or processing performed other than in accordance with paragraph 103b), all internal storage and circuitry shall either be cleared of classified data and verified by a responsible individual designated in the SPP or disconnected. In addition, all media on which classified data has been recorded shall be removed or disconnected or properly stored or cleared. Area controls shall remain in effect except as specified in paragraph 103b(1).

104. Clearance of Main Memory, Other Magnetic Media, and Equipment

a. In a controlled ADP environment, each memory location, register and other internal circuitry used for the storage of classified data shall be overwritten or otherwise cleared once when no longer required, before reutilization, or before the content of the memory location, register, or internal circuitry may

be read to preclude the unauthorized disclosure of classified data. Acceptable methods to accomplish the above are by program instruction, clear switch action, or power-on reset cycle or a combination of these methods. Verification of the clearance action will be accomplished to insure that all applicable portions of memory have been cleared.

b. Magnetic media on which classified information has been recorded shall be disconnected and properly stored, or shall be declassified in accordance with paragraphs 105a and b. Discs and drums which have been overwritten once with unclassified data may be utilized for processing data in an unclassified mode, but they will be handled and accounted for in accordance with the highest classification of information ever recorded thereon until the medium or device is declassified in accordance with paragraph 105. Magnetic media containing operational COMSEC keying material may not be cleared for reuse by the above procedure and must retain their classification until properly destroyed.

c. Should memory units or magnetic storage media be removed from the controlled environment, the provisions of paragraph 105 apply.

d. Punch card or card reader equipment must be physically examined as a part of the process of clearing the equipment of classified information. This will include visual examination of the normal card path through the equipment and the operation of the equipment for three or more card cycles with input hopper empty to detect the possible presence of punched cards which have not been processed. In addition, such an examination must include a search of the locations of the equipment where, because of a malfunction, a punched card or portion of a punched card may have become lodged. This procedure necessitates the removal or opening of equipment access panels and/or other removable components to perform a visual inspection.

105. Declassification Procedure

The eventual temporary or outright release of a storage device or a system, including storage media, should be anticipated. Due to the physical properties and retentive capabilities of magnetic media and devices (e.g., cores, drums, discs, tapes) used to store, record or manipulate classified data in a computer system, special precautions must be taken in the release of such media to safeguard possible residual classified information until adequate declassification procedures described below have been executed. Except as authorized below,¹³ all storage media and internal memory on which classified information is magnetically recorded shall be safeguarded and accounted for according to the requirements prescribed in this Manual for the highest level of classified information ever recorded thereon. Procedures for declassification are as follows:

a. Magnetic Tapes. When all classified information has been eradicated from a magnetic tape through the use of degaussing equipment authorized by the cognizant security office,¹⁴ the tape may be handled on an unclassified basis, provided further that:

- (1) All markings identifying previous source, subject matter, use or classification of the information previously recorded thereon are removed;
- (2) The contractor establishes such procedure as is required to insure strict compliance with the manufacturer's instructions for operating the degaussing equipment; and

¹³ For specific guidance regarding the eradication of SIOP, COMSEC and similar type Special Access Program information magnetically recorded on a tape, disc or drum, see the appropriate User Agency publications pertaining to that particular subject matter.

¹⁴ The cognizant security office will, upon request, advise the contractor of currently authorized magnetic tape, card and cassette degaussing equipment and any conditional instructions regarding their use promulgated by HQ DLA. Special instructions issued by manufacturers of approved degaussers must be precisely followed in order to insure complete degaussing. Requests for approval to use other degaussing equipment may be submitted in duplicate to the cognizant security office, including a full description of the equipment and operating procedures.

- (3) The destruction records and certificates required by paragraph 19e are executed upon eradication of the classified information and are maintained at the control station(s) established under paragraph 12.

b. Magnetic Disc, Disc Pack and Drum. Magnetic discs, disc packs, drums and other similar rigid magnetic storage devices shall be overwritten a minimum of three times, once with the binary digit "1", once with the binary digit "0", and once again with a single numeric, alphabetic, or special character (other than blank). When the capability exists as an integral part of the storage subsystem, an AC/DC erase will be applied to all data tracks before the tracks are overwritten. Verification of the overwrite action must be accomplished to insure that the storage device has been declassified. Unclassified data used in the final overwrite shall be left on the device. The current used in overwriting must be equal to that used in recording the information. If the storage device has failed in such a manner that it cannot be overwritten, the device may be declassified by exposing the recording surface(s) to a permanent magnet having a field strength at the recording surface of at least 1,500 OERSTED. Care must be taken to insure the entire surface is wiped at least three times by a nonuniform motion of the magnet. A thin sheet of clear plastic (a 1-5 mil sheet) should be used to prevent damage to the recording surface(s).

c. Magnetic Core. Magnetic core must be declassified by setting each addressable memory location alternately to all "ones" and all "zeros" for 1000 cycles until the state is changed at least 999 times.

d. Thin Film and Plated Wire. Non-mechanical flat thin film and plated wire memories which have been used to store classified data may be declassified after recording unclassified data in all storage locations and allowing such data to remain on the device for 72 hours at temperatures matching or exceeding those extant during

the period of classified storage. Other types of thin film memories must be handled on a case-by-case basis with provision of full details to the cognizant security office.

e. Magnetic Storage Media Used to Store Analog, Video, or Similar Non-Digital Information. Magnetic tape may be declassified by degaussing as in paragraph 105a. Rigid magnetic storage surfaces may be declassified as in paragraph 105b, except that the unclassified overwriting signal must be analog instead of binary. The overwrite recording must be left intact on the device. In the case of failure of the degausser or overwriting methods, a permanent magnet must be used as in paragraph 105b, for rigid recording devices.

f. Printer Ribbons. Printer ribbons shall be considered declassified when they have been cycled through the printer and the information is obliterated. In no case will this be less than five cycles. "One-time" printer ribbons may be handled as classified waste as provided in paragraph 19.

g. Destruction Certificates. Destruction certificates must be executed and retained in accordance with paragraph 19.

h. Records of Release. Records of release of declassified storage media shall be maintained for a period of 2 years after disposition of the device or equipment.

106. Dedicated Mode

There are three conditions normally encountered when considering processing data in a dedicated mode; (i) self-contained, (ii) intra-complex, and (iii) inter-complex.

a. Self-Contained. In this type of condition all operations take place within the controlled Central Computer Facility. All remote terminals must be disconnected.

b. Intra-Complex and Inter-Complex. In these situations all classified data processing

takes place within the controlled Central Computer Facility, and in controlled areas housing remote terminals. Transmission to and/or from such terminals and the computer must be in conformance with paragraph 107. All other remote terminals, regardless of location must be disconnected. Requests for approval to use either of these "Dedicated Mode" type systems shall be submitted in writing to the cognizant security office and shall include a complete description of the ADP system, including the category of classified information to be processed. Included in the request should be a description of procedures for:

- (1) Personnel and physical controls (see paragraph 103) and of the procedural and administrative security controls to be placed in effect for the ADP system and for each location where a remote terminal is connected.
- (2) Transmission Controls. If the transmission is by means other than approved CRYPTOGRAPHIC systems, a complete description of the in-depth physical controls of the transmission lines is to be included.
- (3) Authentication of each authorized user or group of users. One acceptable method would be the use of a unique random six alphanumeric character password classified the same as the highest category of information to which the user (or group) is authorized access in the system. Such a password would need to be changed at least every 3 months and upon termination or reassignment of any user possessing knowledge of the password or when the password is believed to have been compromised or subjected to compromise. To further improve the reliability of the procedure for identification of the user (or group) individual identification devices may be used in conjunction with the six alphanumeric character password iden-

DoD 5220.22-M

tification procedure. This can include the entry into the system of a series of facts from the individual's personal background which generally would not be information known to anyone else, and which would be called up on a random basis and would require a specific answer by the user. Other augmenting individual identification devices, such as the use of hand geometry (fingerprint scanner or hand scanner), voice or signature comparison devices may also be utilized as additional safeguards to supplement access control procedures.

- (4) An SPP detailing the exact procedures the contractor will employ in operating the proposed system.
- (5) Other security factors that have a bearing and which will assist in an evaluation of the overall system. The contractor's proposed system must include provisions for control of the entire complex.

107. Transmission

Classified data may be transmitted as follows:

a. Inter-Complex. Only over approved CRYPTOGRAPHIC communication circuits, and only with the prior written approval and in accordance with instructions of the contracting officer.

b. Intra-Complex. Over approved CRYPTOGRAPHIC communication circuits with the prior written approval and in accordance with the instructions of the contracting officer. In the event the contracting officer advises that CRYPTOGRAPHIC equipment is not available, other approved circuits may be used with the prior written approval of

the cognizant security office. Such circuits must be protected by an in-depth physical security system and include the following:

- (1) *Dedicated Lines.* The transmission line(s) must be dedicated to the computer and the remote terminal(s). A remote terminal(s) must be approved for the handling of classified data. A transmission line(s) shall be dedicated to computer/terminal traffic and be separated from and not included in a cable which contains other lines not dedicated to the transmission of classified data. The line may not be connected to or through telephone frames, switching equipment or any other telephone equipment.
- (2) *Line Surveillance.* The transmission lines should all remain in secure areas certified for the safeguarding of the highest level of classified information transmitted. In the event these lines cannot be contained entirely within secure areas, continual surveillance as defined below must be maintained. Surveillance must be accomplished by one of the following: (i) alarming the transmission line itself with an alarm system which will provide a central station response time which is not greater than 15 minutes, and by conducting checks of the line and alarm integrity at least once daily; or (ii) continual surveillance of the lines by appropriately cleared guards, indoctrinated as to the significance of the lines. Indoctrination must be sufficient to enable the guards to detect attempts to compromise the security of the system, and to determine the action to be taken in the event of compromise or suspected compromise; or (iii) a combination of protected transmission lines and guard patrols, in which event the frequency of guard patrols will be determined by the degree of line protection and any other pertinent security features.

- (3) Physical Security and Terminal Stations. As a general rule, the physical security of the line terminal blocks and repeater stations should, as a minimum, be equal to a strongroom (paragraph F, Appendix IV). Supplemental controls shall provide for either an alarm system with a 15-minute control station response time or irregularly scheduled hourly patrols. Junction boxes and manholes should be secured and locked with a three-position, dial type, changeable combination lock.

108. Subcontracting Classified Data Processing

a. Processing by Subcontractor. A contractor may subcontract with another cleared contractor on an exclusive-use basis for the processing of classified data. Subcontracting under this category encompasses job shops which process individual jobs on an "across-the-counter" basis, and subcontractors who provide the complete software package as well as the actual processing of the classified programs. The provisions of this Section and Section VI apply. After processing any classified data for a contractor, the subcontractor shall clear and verify the memory of the computer and all other addressable areas on which classified data has been recorded prior to processing any data for another contractor.

b. Use of an ADP System on a Leased Basis (see paragraph 5b). A contractor may use the ADP system of another cleared contractor on a leased, exclusive-use basis (facilities which rent time on computers are often classed "service centers" or "service bureaus"), provided:

- (1) The lessor is responsible for assuring that the integrity of the ADP system is maintained at all times;
- (2) The using contractor establishes ade-

quate physical and personnel security controls, including provisions for clearing the equipment of the classified data prior to relinquishing physical control, and the incorporation of such procedures in his SPP (or supplement thereto); and

- (3) The cognizant security office approves such procedures. Prior to granting approval, the cognizant security office shall assure that adequate security measures will be placed into effect by the using contractor while classified data is being processed, and that residual classified information will not be retained in the ADP system. In many instances, a representative of the lessor contractor remains in the computer area during the run for equipment maintenance purposes. The using contractor therefore is responsible for insuring that the lessor's employee has the appropriate clearance and need-to-know. In addition, all classified material belonging to the using contractor shall be removed from the lessor's premises at the end of the lease period.

109 Audit Trail

Unauthorized attempts to change, circumvent, or otherwise violate security features of the Operating System should be detectable and reported within a known time by the Operating System, causing an abort or suspension of the responsible user activity. In addition, the incident shall be recorded in the audit log, and the ADP system security supervisor shall be notified. An audit log or file (manual, machine or a combination of both) shall be maintained as a history of the use of the ADP system to permit a regular security review of system classified activity. The log should record as a minimum security related transactions, including each access to a classified file and the nature of the access (e.g., log-ins, production of ac-

countable classified outputs and creation of new classified files, start/stop time of process, identity of user, files deleted, file classification and processing anomalies). Each classified file successfully accessed, regardless of the number of individual references, during each "job" or "interactive session" will also be recorded in the audit log. The ADP security supervisor shall review the log at least weekly to assure that all pertinent activity is properly recorded and that appropriate action has been taken to correct any anomaly.

110. Multi-Level Resource-Sharing Systems

The objective of this paragraph is to provide guidelines and establish techniques and procedures which can be used to secure resource-sharing ADP systems for the multi-level security mode so that, with reasonable dependability, deliberate or inadvertent ac-

cess to classified material by unauthorized personnel or the unauthorized manipulation of the computer and its associated peripheral devices, which could lead to the compromise of classified information can be prevented. A number of hardware and software requirements are being developed. However, an essential element necessary for decision by the approving authority is the security testing and evaluation of such systems. Security testing and evaluation techniques are under development by the Government. Pending the development and implementation of testing and evaluation, approval to use resource-sharing ADP systems for processing classified information in the multi-level security mode is being held in abeyance. Requests for exceptions to the dedicated security mode of operation, along with full descriptive details, including a general SPP, must be submitted 90 days prior to proposed start of operation to the cognizant security office for case-by-case consideration.

APPENDIX I

INDUSTRIAL SECURITY FORMS

A. Application

The purpose of this Appendix is to describe the forms used by DoD contractors in industrial security matters and to provide instructions for the use and completion of each. A copy of each form is included. These forms shall not be used for any purpose or in any other manner except as provided for in this Manual or for training purposes.

B. Department of Defense Personnel Security Questionnaire (Industrial) (DD Form 48)

This form is used to obtain personal data

from a U.S. citizen being considered for a DoD CONFIDENTIAL or SECRET personnel security clearance. The form is prepared jointly by management and the person being considered for the clearance. The submission of this form shall not be required except where the person concerned is being processed for a clearance. The completed form should be forwarded to the DISCO, P.O. Box 2499, Columbus, Ohio 43216. However, forms which pertain to OODEPs and which are submitted in conjunction with the facility security clearance application, or as a change thereto, shall be mailed to the cognizant security office. ←

DEPARTMENT OF DEFENSE PERSONNEL SECURITY QUESTIONNAIRE (INDUSTRIAL)		FORM APPROVED OMB NO. 22-R046	DATE
DD FORM 48 1 JAN 74 USE 1 JUL 69 EDITION UNTIL EXHAUSTED PART I	1. LAST NAME - FIRST NAME - MIDDLE NAME		2. SEX
	3. ALIASES AND ALL FORMER NAMES		4. SOCIAL SECURITY NUMBER
	5. MONTH, DAY, YEAR OF BIRTH	6. PLACE OF BIRTH	7. SERVICE NUMBER
<p>INSTRUCTIONS TO EMPLOYEE: DO NOT FILL IN ANY PORTION OF THIS FORM UNLESS YOU ARE EMPLOYED AND ON THE PAYROLL OF THE EMPLOYER FROM WHOM YOU RECEIVE THIS FORM. This form is in four (4) parts. Part II must be completed by your employer before you complete the other parts. You must complete Part III in private. Before filling in any part, you should familiarize yourself with all questions. Do not sign this form without first reading the instructions in Part IV.</p> <p>TYPE OR PRINT ALL ANSWERS. If more space is required, attach additional sheets, identifying by corresponding block number. FORM WILL NOT BE ACCEPTED UNLESS COMPLETELY AND PROPERLY EXECUTED. Questions which do not apply shall be marked "None."</p>			
8. RELATIVES		DATE AND PLACE OF BIRTH	CITIZENSHIP
a. FATHER			
b. MOTHER (Full Maiden Name)			
c. SPOUSE (Full Maiden Name)			
9. RESIDENCES (List all from 18th birthday or during past 15 years, whichever is shorter. If under 18, list present and most recent addresses.)			
a. FROM	b. TO	c. NUMBER AND STREET	d. CITY
			e. STATE
10. EMPLOYMENT (List all from 18th birthday or during past 15 years, whichever is shorter. If under 18, list present and most recent employment)			
a. FROM	b. TO	c. EMPLOYER	d. PLACE
11. LAST CIVILIAN SCHOOL			
a. FROM	b. TO	c. NAME	d. PLACE
PART II (TO BE COMPLETED BY EMPLOYER)			
TO:		NAME AND ADDRESS OF EMPLOYER (If a subsidiary, include name of parent company)	
Defense Industrial Security Clearance Office Defense Supply Agency Box 2499 Columbus, Ohio 43216			
JOB TITLE AND DESCRIPTION OF EMPLOYEE'S DUTIES WHICH REQUIRE ACCESS TO CLASSIFIED INFORMATION		CONTRACT NUMBER, WHEN APPLICABLE	
		SECURITY CLASSIFICATION OF MATERIALS OR INFORMATION EMPLOYEE WILL HAVE ACCESS TO	
I CERTIFY THAT THE ENTRIES MADE BY ME ABOVE ARE TRUE, COMPLETE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF AND ARE MADE IN GOOD FAITH.		SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE	

PART I (Continued)					
12. EDUCATION (Account for all civilian and military academies)					
YEARS (Month if known)		NAME AND LOCATION OF SCHOOL	GRADUATE		DEGREE
FROM	TO		YES	NO	
13. CITIZENSHIP					
ARE YOU A CITIZEN OF THE UNITED STATES? <input type="checkbox"/> YES <input type="checkbox"/> NO (If answer is "YES", complete Item a and b or c, if appropriate. If answer is "NO", do not complete this form. Obtain DD Form 49 from your employer.)					
a. I AM A CITIZEN OF THE UNITED STATES BY REASON OF: <input type="checkbox"/> BY BIRTH IN THE UNITED STATES <input type="checkbox"/> BY NATURALIZED CITIZENSHIP * <input type="checkbox"/> BY BIRTH IN A FOREIGN COUNTRY OF UNITED STATES PARENTS <input type="checkbox"/> BY DERIVATIVE CITIZENSHIP *					
* If checked complete either "Citizenship by Naturalization" or "Citizenship by Derivation" Section below.					
b. CITIZENSHIP BY NATURALIZATION*					
WHERE NATURALIZED (City, County, State)			DATE NATURALIZED		
COURT			CERTIFICATE NUMBER		
c. CITIZENSHIP BY DERIVATION *					
PARENT'S NAME			PARENT'S CERTIFICATE NUMBER		
14. ORGANIZATIONAL MEMBERSHIP					
LIST ALL ORGANIZATIONS EXCEPT LABOR UNIONS AND EXCEPT ORGANIZATIONS REFERRED TO IN ITEM 27 BELOW IN WHICH YOU HOLD OR HAVE HELD MEMBERSHIP. IF NONE, SO STATE.					
NAME AND ADDRESS	TYPE	OFFICE HELD	FROM (Date)	TO (Date)	
15. MILITARY SERVICE					
a. COUNTRY	BRANCH OF SERVICE	SERVICE NUMBER	FROM (Date)	TO (Date)	
b. ARE YOU A MEMBER OF A RESERVE COMPONENT? <input type="checkbox"/> YES <input type="checkbox"/> NO (If answer is "YES", furnish service, component and current status under Item 21, "Remarks".)					
c. LOCAL DRAFT BOARD (United States) AND ADDRESS			d. SELECTIVE SERVICE NO.	e. CLASSIFICATION	
16. PREVIOUS CLEARANCE					
a. HAVE YOU EVER BEEN PREVIOUSLY GRANTED A SECURITY CLEARANCE? (If answer is "YES", indicate level of clearance, when granted, by whom and where employed at that time under Item 21, "Remarks".) <input type="checkbox"/> YES <input type="checkbox"/> NO					
b. HAVE YOU EVER TERMINATED EMPLOYMENT WHILE A REQUEST OR APPLICATION FOR A SECURITY CLEARANCE WAS PENDING? (If answer is "YES", furnish name and address of employer under "Remarks". If termination resulted from a reduction in force, so indicate and furnish details under "Remarks". If you since have been granted a clearance by the Government, indicate under Item 21, "Remarks" the date, level of clearance and where employed.) <input type="checkbox"/> YES <input type="checkbox"/> NO					

DoD 5220.22-M

7. OTHER RELATIVES				
a. LIST CHILDREN, BROTHERS, SISTERS (16 years and older) AND FORMER SPOUSE(S)				
RELATION	NAME IN FULL	ADDRESS (Enter "deceased" if no longer living)	PLACE AND DATE OF BIRTH	PRESENT CITIZENSHIP
b. LIST OTHER LIVING RELATIVES AND RELATIVES OF SPOUSE WHO ARE NOT UNITED STATES CITIZENS.				
18. FOREIGN COUNTRIES VISITED OR RESIDED IN				
CITY AND COUNTRY	DATE LEFT U.S.	DATE RETURNED U.S.	PURPOSE AND TYPE OF VISA	
19. LIST EACH FOREIGN GOVERNMENT, FIRM, CORPORATION OR PERSON FOR WHOM YOU ACT OR HAVE ACTED AS A REPRESENTATIVE, OFFICIAL OR EMPLOYEE IN THE PAST 5 YEARS. LIST ALL COMMUNIST GOVERNMENTS, FIRMS OR CORPORATIONS FOR WHOM YOU HAVE EVER ACTED IN SUCH CAPACITY. ATTACH A STATEMENT, AS REQUIRED BY PARAGRAPH 20K, 15M, FULLY DESCRIBING EACH AFFILIATION. (If none, so indicate.)				
20. REFERENCES (Give five personal references, stating business address of all references, if known. Do not include relatives, former employers, or persons living outside the United States.)				
NAME	YEARS KNOWN	STREET AND NUMBER	CITY	STATE
21. REMARKS (If additional space is needed, continue on plain paper.)				

(COMPLETE PARTS III AND IV ON REVERSE SIDE OF ORIGINAL COPY)

DoD 5220.22-M

<p>FURTHER INSTRUCTIONS: DO NOT COMPLETE PARTS III OR IV AT THIS TIME. Return this partially completed form to your employer who will review it to assure all entries are complete and the form is properly filled in. After return, proceed with completion of Parts III and IV.</p>		
<p>PART III</p>		
<p>Complete the items below in private. The answers or statements in this part are privileged information between you and the Government. You should enter in Item 28 any information relating to your answers which might require further explanation, or any additional information which may have a bearing on your security clearance.</p>		
<p>22. HAVE YOU EVER BEEN ARRESTED, CHARGED, OR HELD BY ANY LAW ENFORCEMENT AUTHORITIES FOR ANY VIOLATION OF ANY LAW, REGULATION OR ORDINANCE? INCLUDE ALL COURTS-MARTIAL. DO NOT INCLUDE ANYTHING THAT HAPPENED BEFORE YOUR 16TH BIRTHDAY. DO NOT INCLUDE TRAFFIC VIOLATIONS FOR WHICH THE ONLY PENALTY IMPOSED WAS A FINE OF \$25.00 OR LESS. ALL OTHER CHARGES MUST BE INCLUDED EVEN IF THEY WERE DISMISSED.</p> <p><input type="checkbox"/> YES <input type="checkbox"/> NO IF "YES", GIVE DATE AND PLACE, CHARGE, AND DISPOSITION:</p>		
<p>23. WHAT TYPE OF DISCHARGE DID YOU RECEIVE, IF ANY, FROM MILITARY SERVICE?</p>		
<p>24. HAVE YOU EVER HAD A SECURITY CLEARANCE SUSPENDED, DENIED, OR REVOKED? (If answer is "YES", indicate level of clearance, when suspended, denied or revoked, by whom and where employed under Item 28, "Remarks". If you since have been granted a clearance by the government, indicate under Item 28, "Remarks", the date, level of clearance and activity which restored the clearance.)</p> <p><input type="checkbox"/> YES <input type="checkbox"/> NO</p>		
25.	YES	NO
a. DO YOU HAVE A HISTORY OF MENTAL OR NERVOUS DISORDERS?		
b. ARE YOU NOW OR HAVE YOU EVER BEEN ADDICTED TO THE USE OF HABIT FORMING DRUGS SUCH AS NARCOTICS OR BARBITURATES?		
c. ARE YOU NOW OR HAVE YOU EVER BEEN A CHRONIC USER TO EXCESS OF ALCOHOLIC BEVERAGES?		
<p>(If answer to any of the above is "YES", explain. Give names and addresses of hospitals, clinics, sanatoriums, and physicians who have examined or treated you for such conditions.)</p>		
<p>26. AUTHORITY TO RELEASE MEDICAL INFORMATION</p> <p>I HEREBY GRANT PERMISSION TO THE DEPARTMENT OF DEFENSE TO OBTAIN AND REVIEW COPIES OF MY MEDICAL AND INSTITUTIONAL RECORDS RELATING TO CONDITIONS LISTED IN ITEM 25 AND TO QUESTION THOSE WHO HAVE EXAMINED OR TREATED ME THEREFOR.</p>		
SIGNATURE OF EMPLOYEE		DATE
27.	YES	NO
<p>ORGANIZATIONAL MEMBERSHIP</p>		
a. ARE YOU NOW, OR HAVE YOU EVER BEEN, A MEMBER OF THE COMMUNIST PARTY, U.S.A., THE COMMUNIST POLITICAL ASSOCIATION, THE YOUNG COMMUNIST LEAGUE, OR ANY COMMUNIST ORGANIZATION?		
b. ARE YOU NOW OR HAVE YOU EVER BEEN A MEMBER OF ANY FOREIGN OR DOMESTIC ORGANIZATION, ASSOCIATION, MOVEMENT, GROUP, OR COMBINATION OF PERSONS WHICH IS TOTALITARIAN, FASCIST, COMMUNISTIC, OR SUBVERSIVE, OR WHICH HAS ADOPTED, OR SHOWS, A POLICY OF ADVOCATING OR APPROVING THE COMMISSION OF ACTS OF FORCE OR VIOLENCE TO DENY OTHER PERSONS THEIR RIGHTS UNDER THE CONSTITUTION OF THE UNITED STATES OR WHICH SEEKS TO ALTER THE FORM OF GOVERNMENT OF THE UNITED STATES BY UNCONSTITUTIONAL MEANS?		
<p>IF YOUR ANSWER TO EITHER OF THE ABOVE QUESTIONS IS "YES", LIST IN ITEM 28, THE NAMES OF ALL SUCH ORGANIZATIONS, ASSOCIATIONS, MOVEMENTS, GROUPS OR COMBINATION OF PERSONS AND DATES OF MEMBERSHIP. GIVE COMPLETE DETAILS OF YOUR ACTIVITIES THEREIN AND MAKE ANY EXPLANATION YOU DESIRE REGARDING YOUR MEMBERSHIP OR ACTIVITIES.</p>		
<p>28. REMARKS (Use the space provided below and attach additional sheets, if necessary.)</p>		

PART IV		
<p>IMPORTANT NOTICE: Your signature on the following certification must be witnessed; the witness may be an employee of your firm. Prior to affixing your signature to the form, remove all carbons, fold the form so that the witness to your signature will not see any portion of Part III of the completed Personnel Security Questionnaire. Sign and date the form in the presence of the witness. Have the witness affix his signature and his address to the appropriate blocks on the form.</p>		
<p>NOTE: PENALTY FOR MISREPRESENTATION. Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false, or partial answers) may serve as a basis for denial of clearance for access to classified Department of Defense information. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of 5 years imprisonment, \$10,000 fine, or both, knowingly and willfully to make a false statement or representation to any Department or Agency of the United States as to any matter within the jurisdiction of any Department or Agency of the United States.</p> <p><i>This includes any statement knowingly and willfully made by employer or employee herein which is knowingly incorrect, incomplete or misleading in any important particular. Title 18 United States Code 911 states "whoever falsely and willfully represents himself to be a citizen of the United States shall be fined not more than \$1,000 or imprisoned not more than three years, or both".</i></p>		
<p align="center"><u>CERTIFICATION</u></p> <p>WARNING: Read every sentence of the Certification before signing. I certify that my above answers are true, complete, and correct to the best of my knowledge and belief, and are made in good faith. I certify that I know that any misrepresentation or false statement made by me herein may subject me to prosecution under Section 1001 of the United States Criminal Code, with penalties up to five (5) years imprisonment and \$10,000 fine, and provide a basis for denial of security clearance. I certify that I have read and understand each sentence of this Certification.</p>		
SIGNATURE OF WITNESS	SIGNATURE OF EMPLOYEE	DATE OF SIGNATURE
ADDRESS OF WITNESS (City, County, State)		
<p align="center"><u>INSTRUCTIONS TO EMPLOYEE UPON COMPLETION OF ABOVE</u></p> <p>Now that the form is signed and witnessed, place it in the pre-addressed envelope furnished (DSA Form 703), together with the completed FD Form 258 (Fingerprint Card), seal the envelope, sign across the envelope flap on the line provided, and affix the date of signature. Deliver the sealed envelope to your employer immediately.</p>		

**C. Application and Authorization for
Access to Confidential Information
(DD Form 48-2)**

This form is used to obtain personal data from a U.S. citizen being considered for a CONFIDENTIAL personnel security clearance by a contractor. The form is prepared jointly by the person being considered for

the clearance and by the contractor. Completion of this form is a prerequisite to the granting of a CONFIDENTIAL clearance by a contractor. The use of this form is not retroactive in the case of employees who previously were granted a CONFIDENTIAL clearance by the contractor, so long as they are continuously employed by the same contractor or there has been no break in employment in excess of 12 months.

APPLICATION AND AUTHORIZATION FOR ACCESS TO CONFIDENTIAL INFORMATION (INDUSTRIAL)		TYPE OR PRINT ALL ANSWERS	Form Approved OMB No. 22-R230	
<p>NOTE: PENALTY- Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false, or partial answers) may serve as a basis for denial of clearance for access to classified Department of Defense information. In addition, Title 18 United States Code 1001 makes it a criminal offense, punishable by a maximum of 5 years' imprisonment, \$10,000 fine, or both, knowingly and willfully to make a false statement or representation to any Department or Agency of the United States as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement knowingly and willfully made by employer or employee herein which is knowingly incorrect, incomplete or misleading in any important particular - Title 18 United States Code 911 states "whoever falsely and willfully represents himself to be a citizen of the United States shall be fined not more than \$1,000 or imprisoned not more than three years, or both".</p>				
<p>PURPOSE: The completion of this form is required in the national interest prior to an individual being granted a security clearance for classified information.</p>				
<p>INSTRUCTIONS - This is a three-part form. Part I is an application for access and shall be executed by U.S. citizen employees provided their employer determines that access to Confidential Information is required in the performance of the employee's assigned duties. Part II is the employee's authorization for access to Confidential Information and shall be completed by the employer. Copy of this form shall be maintained by the contractor for all employees granted a security clearance for Confidential Information. Part III is a listing of Communist countries which the employee should refer to when completing Item 11.</p>				
PART I - APPLICATION FOR ACCESS TO CONFIDENTIAL INFORMATION				
TO BE COMPLETED BY EMPLOYEE				
NAME AND ADDRESS OF EMPLOYER				
1. LAST NAME - FIRST NAME - MIDDLE NAME		2. ANY OTHER NAME BY WHICH KNOWN (Alias, maiden or former legal name)		
3. DATE OF BIRTH (Month, Day & Year)		4. PLACE OF BIRTH (City, County, State)		
5. SOCIAL SECURITY NUMBER		6. SEX		
7. HAVE YOU EVER APPLIED FOR OR RECEIVED A SECURITY CLEARANCE? <input type="checkbox"/> YES <input type="checkbox"/> NO				
8. IF THE ANSWER TO ITEM 7 IS "YES", INDICATE BELOW THE LEVEL OF CLEARANCE, WHEN APPLIED FOR, WHEN GRANTED, BY WHOM, AND WHERE EMPLOYED AT THAT TIME.				
9. ORGANIZATIONS WITH WHICH AFFILIATED (past and present) OTHER THAN RELIGIOUS OR POLITICAL ORGANIZATIONS OR THOSE WHICH SHOW RELIGIOUS OR POLITICAL AFFILIATION. (If none, so state)				
10. ARE YOU A CITIZEN OF THE UNITED STATES? <input type="checkbox"/> YES <input type="checkbox"/> NO. (If answer is "Yes", complete the following; if answer is "No", return this form to your employer.)				
<input type="checkbox"/> I AM A CITIZEN OF THE UNITED STATES BY REASON OF MY BIRTH IN THE UNITED STATES <input type="checkbox"/> MY NATURALIZED CITIZENSHIP *				
<input type="checkbox"/> MY BIRTH IN A FOREIGN COUNTRY OF UNITED STATES PARENTS <input type="checkbox"/> MY DERIVATIVE CITIZENSHIP *				
*If checked complete either "Citizenship by Naturalization" or "Citizenship by Derivation" Section below.				
WHERE NATURALIZED (City, County, State)		DATE NATURALIZED		
COURT		CERTIFICATE NO.		
CITIZENSHIP BY DERIVATION *				
PARENT'S NAME		PARENT'S CERTIFICATE NO.		
11. HAVE YOU RESIDED AT ANY TIME DURING THE PAST 15 YEARS OR SINCE YOUR 18TH BIRTHDAY, WHICHEVER IS LATER, IN COMMUNIST COUNTRIES LISTED UNDER PART III? (If answer is "Yes", indicate city and country, dates of residence, under Item 14 "Remarks.") <input type="checkbox"/> YES <input type="checkbox"/> NO				
12. LIST RELATIVES AND RELATIVES OF SPOUSE KNOWN TO BE LIVING IN COMMUNIST COUNTRIES LISTED UNDER PART III.				
RELATION	NAME	ADDRESS	PLACE & DATE OF BIRTH	PRESENT CITIZENSHIP
13. ARE YOU A REPRESENTATIVE OF A FOREIGN INTEREST? <input type="checkbox"/> YES <input type="checkbox"/> NO				
14. REMARKS				

Fold
LineFold
Line

DoD 5220.22-M

INSTRUCTIONS: Read every sentence of the Certification before signing in the presence of a witness who may be a member of your firm. If you cannot sign the certification for any reason, return this form to your employer who will have you complete a different form.

CERTIFICATION

I certify that I have never been, past or present, a member in any organization, association, movement, group, or combination of persons, (1) which advocates the overthrow of our constitutional form of government, (2) or which had adopted a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States, (3) or which seeks to alter the form of Government of the United States by unconstitutional means.

I certify that I know that any misrepresentation or false statement made by me herein may subject me to prosecution under Title 18, United States Criminal Code, Sections 911 and 1001, with penalties up to five (5) years imprisonment and \$10,000 fine.

I certify that I have read and understand each sentence of this Certification.

I certify that the entries made by me on this form are true, complete, and correct to the best of my knowledge and belief, and are made in good faith.

I certify that I am a citizen of the United States.

SIGNATURE OF WITNESS

SIGNATURE OF PERSON MAKING CERTIFICATION

DATE OF SIGNATURE

ADDRESS OF WITNESS (City, County, State)

PART II - AUTHORIZATION FOR ACCESS TO CONFIDENTIAL INFORMATION

TO BE COMPLETED BY EMPLOYER

Whereas the Department of Defense has delegated to its contractors (*employers*) authority to grant access authorization for access to Confidential Information to his employees who require access in the performance of the employee's assigned duties; the undersigned, a duly authorized representative of the contractor, certifies that he has examined Part I of this form and the employment records pertaining to the employee executing Part I of this form, and has determined that: -
(Check the appropriate block(s))

1. The employee is a United States citizen; and that

☐

2. The employee may be granted a security clearance for Confidential information in accordance with the provisions of paragraph 24b, Industrial Security Manual for Safeguarding Classified Information and such authorization is hereby granted this date; and/or

☐

3. The application is required to be referred to the military cognizant security office for determination.

Date _____

By _____
(Signature)

(Name of Contractor)

(Typed name and title of authorized representative)

PART III - LIST OF COMMUNIST COUNTRIES

Albania
Bulgaria
Chinese Peoples Republic (Communist China) (including Tibet)
Cuba
Czechoslovakia
Democratic Peoples Republic of Korea (North Korea)
Democratic Republic of Vietnam (North Vietnam)
German Democratic Republic (GDR) (East Germany, including the Soviet Sector of Berlin)
Hungary
Mongolian Peoples Republic (Outer Mongolia)
Poland
Rumania
Yugoslavia
Kurile Islands
South Sakhalin (Karafuto)
Union of Soviet Socialist Republics (USSR) (including Estonia, Latvia, Lithuania, and all other constituent republics)

DD FORM 48-2
1 APR 74

EDITION OF 1 JAN 68 MAY BE USED UNTIL EXHAUSTED

**D. Department of Defense Personnel
Security Questionnaire (Updating)
(DD Form 48-3)**

This form is used to obtain current and updating personal data to process a clearance action when an individual with a security clearance is transferring employment from one contractor to another contractor within a 12-month period and requires a security clearance in his new employment. It is also

used in converting a User Agency clearance to an industrial security clearance. This form is prepared jointly by management and the individual being processed for the new clearance. In the section to be completed by the employer, the form is addressed to the DISCO, P.O. Box 2499, Columbus, Ohio, 43216. However, forms which pertain to OODEPs which are submitted in conjunction with the facility security clearance application, or as a change thereto, shall be mailed to the cognizant security office.

DEPARTMENT OF DEFENSE PERSONNEL SECURITY QUESTIONNAIRE (UPDATING)		DATE		Form Approved OMB No. 22-R046	
<p>PENALTY - Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false, or partial answers) may serve as a basis for denial of clearance for access to classified Department of Defense information. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of 5 years imprisonment, \$10,000 fine, or both, knowingly and willfully to make a false statement or representation to any Department or Agency of the United States as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly and willfully incorrect, incomplete or misleading in any important particular.</p>					
<p>INSTRUCTIONS: One (1) copy of accomplished form will be submitted by the contractor when prescribed by the Industrial Security Manual for Safeguarding Classified Information to request transfer of clearance. Type or print all answers; form will not be accepted unless completely and properly executed. Use blank sheets for additional information, identifying by item number. Questions which do not apply will be marked "None."</p>					
<p>INSTRUCTIONS TO EMPLOYEE: This form is in three parts. Part I must be completed by your employer before you complete the other parts. You must complete Part III in private. Before filling in any part, you should familiarize yourself with all questions. Do not sign this form without first reading the instructions in Part III.</p>					
PART I					
TO BE COMPLETED BY EMPLOYER					
TO: Defense Industrial Security Clearance Office Defense Supply Agency Box 2499 Columbus, Ohio 43216			NAME AND ADDRESS OF EMPLOYER (If a subsidiary, include name of parent company)		
JOB TITLE AND DESCRIPTION OF EMPLOYEE'S DUTIES WHICH REQUIRE ACCESS TO CLASSIFIED INFORMATION				CONTRACT NUMBER, WHEN APPLICABLE	
				SECURITY CLASSIFICATION OF MATERIALS OR INFORMATION EMPLOYEE WILL HAVE ACCESS TO	
CLEARANCE REQUESTED IS: <input type="checkbox"/> TRANSFER <input type="checkbox"/> CONVERSION <input type="checkbox"/> CONCURRENT					
I CERTIFY THAT THE ENTRIES MADE BY ME ABOVE ARE TRUE, COMPLETE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF AND ARE MADE IN GOOD FAITH				SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE	
PART II					
TO BE COMPLETED BY EMPLOYEE					
1. LAST NAME - FIRST NAME - MIDDLE NAME			2. ANY OTHER NAME BY WHICH KNOWN (Alias, maiden, former legal name; designate which)		
3. DATE OF BIRTH	4a. PLACE OF BIRTH		4b. CITIZEN OF WHAT COUNTRY		
5. SOCIAL SECURITY NUMBER			6. SEX		
7. RESIDENCE (Present Address Only)					
STREET, CITY, STATE OR OTHER POLITICAL SUBDIVISION, AND COUNTRY					FROM (Date)
8. ORGANIZATIONAL MEMBERSHIP (List the name and address of each organization of which you have become a member since the date of your last clearance application. Also show the full name of national organization with which the local organization is affiliated. Under "type" indicate "fraternal," "professional," etc. Do not abbreviate. List the approximate dates of membership if the exact dates are not known. You are not to list labor unions, religious organizations, or political parties. If you do not belong to any organization, enter "none" under the "Name and Address" column.					
NAME AND ADDRESS		TYPE		OFFICE HELD	FROM (Date) TO (Date)
9. LAST EMPLOYMENT (At Which Clearance Was Granted)					
POSITION HELD	EMPLOYER AND IMMEDIATE SUPERVISOR		ADDRESS	FROM (Date)	TO (Date)
10. HAVE YOU EVER BEEN PREVIOUSLY GRANTED A SECURITY CLEARANCE? (If answer is "Yes", indicate level of clearance, when granted, by whom and where employed at that time under Item 12, "Remarks") <input type="checkbox"/> YES <input type="checkbox"/> NO					
11. LIST EACH FOREIGN GOVERNMENT, FIRM, CORPORATION OR PERSON FOR WHOM YOU ACT OR HAVE ACTED AS A REPRESENTATIVE, OFFICIAL OR EMPLOYEE IN THE PAST 5 YEARS. LIST ALL COMMUNIST GOVERNMENTS, FIRMS OR CORPORATIONS FOR WHOM YOU HAVE EVER ACTED IN SUCH CAPACITY. ATTACH A STATEMENT AS REQUIRED BY PARAGRAPH 20k, INDUSTRIAL SECURITY MANUAL, FOR EACH AFFILIATION.					
12. REMARKS					
FURTHER INSTRUCTIONS: Do not complete PART III or the Certification at this time. After completing PART II return the form to your employer who will review it to assure that all entries are complete and the form is filled out properly. After your employer returns the form to you, then start PART III and follow instructions on reverse side.					

DD FORM 48-3
1 FEB 75

EDITION OF 1 JUN 69 MAY BE USED UNTIL EXHAUSTED

PART III														
INSTRUCTIONS: Complete the items below in private. The answers or statements in this Part are privileged information between you and the Government. You should enter in Item 18 below any information relating to your answers which might require further explanation, or any additional information which may have a bearing on your security clearance.														
13. HAVE YOU EVER BEEN ARRESTED, CHARGED, OR HELD BY ANY LAW ENFORCEMENT AUTHORITIES FOR ANY VIOLATION OF ANY LAW, REGULATION, OR ORDINANCE? INCLUDE ALL COURTS-MARTIAL. DO NOT INCLUDE ANYTHING THAT HAPPENED BEFORE YOUR 16TH BIRTHDAY. DO NOT INCLUDE TRAFFIC VIOLATIONS FOR WHICH THE ONLY PENALTY IMPOSED WAS FINE OF \$25.00 OR LESS. ALL OTHER CHARGES MUST BE INCLUDED EVEN IF THEY WERE DISMISSED. (From date of last clearance application) <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <input type="checkbox"/> YES <input type="checkbox"/> NO (If "Yes", give date and place, charge, and disposition.) </div>														
14. WHAT TYPE OF DISCHARGE DID YOU RECEIVE, IF ANY, FROM MILITARY SERVICE? <div style="height: 30px; border: 1px solid black; margin-top: 5px;"></div>														
15. HAVE YOU EVER HAD A SECURITY CLEARANCE SUSPENDED, DENIED, OR REVOKED? (If answer is "Yes", indicate under Item 18 below, the level of clearance, when suspended, denied, or revoked, by whom, and where employed. If you since have been granted a clearance by the Government, indicate under Item 18 below, the date, level of clearance, and the activity which restored the clearance.) <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <input type="checkbox"/> YES <input type="checkbox"/> NO </div>														
16. <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 80%;"></th> <th style="width: 10%; text-align: center;">YES</th> <th style="width: 10%; text-align: center;">NO</th> </tr> </thead> <tbody> <tr> <td>a. DO YOU HAVE A HISTORY OF MENTAL OR NERVOUS DISORDERS?</td> <td></td> <td></td> </tr> <tr> <td>b. ARE YOU NOW OR HAVE YOU EVER BEEN ADDICTED TO THE USE OF HABIT FORMING DRUGS SUCH AS NARCOTICS OR BARBITURATES?</td> <td></td> <td></td> </tr> <tr> <td>c. ARE YOU NOW OR HAVE YOU EVER BEEN A CHRONIC USER TO EXCESS OF ALCOHOLIC BEVERAGES?</td> <td></td> <td></td> </tr> </tbody> </table> <p style="font-size: small; margin-top: 5px;">(If answer to any of the above is "YES", explain. Give names and addresses of hospitals, clinics, sanitoriums, and physicians who have examined or treated you for such conditions.)</p>				YES	NO	a. DO YOU HAVE A HISTORY OF MENTAL OR NERVOUS DISORDERS?			b. ARE YOU NOW OR HAVE YOU EVER BEEN ADDICTED TO THE USE OF HABIT FORMING DRUGS SUCH AS NARCOTICS OR BARBITURATES?			c. ARE YOU NOW OR HAVE YOU EVER BEEN A CHRONIC USER TO EXCESS OF ALCOHOLIC BEVERAGES?		
	YES	NO												
a. DO YOU HAVE A HISTORY OF MENTAL OR NERVOUS DISORDERS?														
b. ARE YOU NOW OR HAVE YOU EVER BEEN ADDICTED TO THE USE OF HABIT FORMING DRUGS SUCH AS NARCOTICS OR BARBITURATES?														
c. ARE YOU NOW OR HAVE YOU EVER BEEN A CHRONIC USER TO EXCESS OF ALCOHOLIC BEVERAGES?														
17. AUTHORITY TO RELEASE MEDICAL INFORMATION I hereby grant permission to the Department of Defense to obtain and review copies of my medical and institutional records relating to conditions listed in Item 16 and to question those who have examined or treated me therefore. <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <tr> <td style="width: 60%;">SIGNATURE OF EMPLOYEE</td> <td style="width: 40%;">DATE</td> </tr> <tr> <td style="height: 40px;"></td> <td></td> </tr> </table>			SIGNATURE OF EMPLOYEE	DATE										
SIGNATURE OF EMPLOYEE	DATE													
18. REMARKS <div style="height: 100px; border: 1px solid black; margin-top: 5px;"></div>														
IMPORTANT NOTICE: Your signature on the following certification must be witnessed; the witness may be an employee of your firm. Prior to affixing your signature to the form, fold the form so that the witness to your signature will not see any portion of Part III of the completed Personnel Security Questionnaire. Sign and date the form in the presence of the witness. Have the witness affix his signature and his address to the appropriate blocks on the form.														
CERTIFICATION														
WARNING: Read every sentence of the Certification before signing. I certify that my above answers are true, complete, and correct to the best of my knowledge and belief, and are made in good faith. I certify that I know that any misrepresentation or false statement made by me herein may subject me to prosecution under Section 1001 of the United States Criminal Code, with penalties up to five (5) years' imprisonment and \$10,000 fine, and provide a basis for denial of security clearance. I certify that I have read and understand each sentence of the Certification.														
SIGNATURE OF WITNESS	SIGNATURE OF EMPLOYEE	DATE OF SIGNATURE												
ADDRESS OF WITNESS (City, County, State)														
INSTRUCTIONS TO EMPLOYEE UPON COMPLETION OF ABOVE CERTIFICATION When the form is signed and witnessed, place the completed form into the pre-addressed envelope furnished, (DSA Form 703), seal the envelope, sign across the envelope flap on the line provided, and affix the date of signature. Deliver the sealed envelope to your employer immediately.														

**E. Department of Defense Personnel
Security Questionnaire (Industrial)
(Multiple Purpose). (DD Form 49)**

This form shall be used in making application for:

a. A U.S. citizen being considered for a TOP SECRET personnel security clearance.

→ *b.* A U.S. citizen being considered for any level of clearance when the individual advises he (she) is a representative of a foreign interest.

c. A U.S. citizen who has relatives or rela-

tives of his spouse who are residing in Communist countries.

d. An immigrant alien being considered for a personnel security clearance.

e. A citizen of Canada or the U.K. being processed for a Reciprocal clearance. The form is prepared jointly by management and the person being considered for clearance. In the section to be completed by the employer, the form should be addressed to the DISCO, P.O. Box 2499, Columbus, Ohio 43216. However, forms which pertain to OODEPs and which are submitted in conjunction with the facility security clearance application, or as a change thereto, shall be mailed to the cognizant security office.

DEPARTMENT OF DEFENSE PERSONNEL SECURITY QUESTIONNAIRE (INDUSTRIAL) (Multiple Purpose)		FORM APPROVED OMB NO. 22-R003	DATE
DD FORM 1 FEB 74 49 USE 1 JUL 69 EDITION UNTIL EXHAUSTED PART I	1. LAST NAME - FIRST NAME - MIDDLE NAME		2. SEX
	3. ALIAS(ES) AND ALL FORMER NAME(S)		4. SOCIAL SECURITY NUMBER
5. MONTH, DAY, YEAR OF BIRTH	6. PLACE OF BIRTH		7. SERVICE NUMBER
<p>INSTRUCTIONS TO EMPLOYEE: DO NOT FILL IN ANY PORTION OF THIS FORM UNLESS YOU ARE EMPLOYED AND ON THE PAYROLL OF THE EMPLOYER FROM WHOM YOU RECEIVE THIS FORM. This form is in four (4) parts. Part II must be completed by your employer before you complete the other parts. You must complete Part III in private. Before filling in any part, you should familiarize yourself with all questions. Do not sign this form without first reading the instructions in Part IV.</p> <p>TYPE OR PRINT ALL ANSWERS. If more space is required, attach additional sheets, identifying by corresponding block number. FORM WILL NOT BE ACCEPTED UNLESS COMPLETELY AND PROPERLY EXECUTED. Questions which do not apply shall be marked "None."</p>			
8. RELATIVES		DATE AND PLACE OF BIRTH	CITIZENSHIP
a. FATHER			
b. MOTHER (Full Maiden Name)			
c. SPOUSE (Full Maiden Name)			
9. RESIDENCES (List all from 18th birthday or during past 15 years, whichever is shorter. If under 18, list present and most recent addresses.)			
a. FROM	b. TO	c. NUMBER AND STREET	d. CITY
			e. STATE
10. EMPLOYMENT (List all from 18th birthday or during past 15 years, whichever is shorter. If under 18, list present and most recent employment)			
a. FROM	b. TO	c. EMPLOYER	d. PLACE
11. LAST CIVILIAN SCHOOL			
a. FROM	b. TO	c. NAME	d. PLACE
PART II (TO BE COMPLETED BY EMPLOYER)			
TO: Defense Industrial Security Clearance Office Defense Supply Agency Box 2499 Columbus, Ohio 43216		NAME AND ADDRESS OF EMPLOYER (If a subsidiary, include name of parent company)	
JOB TITLE AND DESCRIPTION OF EMPLOYEE'S DUTIES WHICH REQUIRE ACCESS TO CLASSIFIED INFORMATION		CONTRACT NUMBER, WHEN APPLICABLE	
		SECURITY CLASSIFICATION OF MATERIALS OR INFORMATION EMPLOYEE WILL HAVE ACCESS TO	
IF SUBJECT IS AN IMMIGRANT ALIEN, HAS HE PRESENTED ALIEN REGISTRATION RECEIPT CARD (Form I-151)? <input type="checkbox"/> YES <input type="checkbox"/> NO			
I CERTIFY THAT THE ENTRIES MADE BY ME ABOVE ARE TRUE, COMPLETE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF AND ARE MADE IN GOOD FAITH.		SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE	

PART I (Continued)					
12. EDUCATION (Account for all civilian schools and military academies)					
YEARS (Month if known)		NAME AND LOCATION OF SCHOOL	GRADUATE		DEGREE
FROM	TO		YES	NO	
13. CITIZENSHIP					
ARE YOU A CITIZEN OF THE UNITED STATES? <input type="checkbox"/> YES <input type="checkbox"/> NO (If answer is "YES", complete Item a and b or c, if appropriate. If answer is "NO", complete item d.)					
a. I AM A CITIZEN OF THE UNITED STATES BY REASON OF: <input type="checkbox"/> BY BIRTH IN THE UNITED STATES <input type="checkbox"/> BY NATURALIZED CITIZENSHIP* <input type="checkbox"/> BY BIRTH IN A FOREIGN COUNTRY OF UNITED STATES PARENTS <input type="checkbox"/> BY DERIVATIVE CITIZENSHIP*					
* If checked complete either "Citizenship by Naturalization" or "Citizenship by Derivation" Section below.					
b. CITIZENSHIP BY NATURALIZATION*					
WHERE NATURALIZED (City, County, State)				DATE NATURALIZED	
COURT				CERTIFICATE NUMBER	
c. CITIZENSHIP BY DERIVATION*					
PARENT'S NAME				PARENT'S CERTIFICATE NUMBER	
d. IMMIGRANT ALIENS ONLY COMPLETE THIS ITEM. U. S. CITIZENS SEE ITEM 13a.					
(1) ALIEN REGISTRATION NO.		(2) CITIZEN OF WHAT COUNTRY		(3) DATE AND PLACE OF LAST ENTRY INTO U. S.	
(4) DATE PETITION OF NATURALIZATION FILED		(5) DATE AND COURT OF ISSUANCE			(6) NUMBER
(7) DO YOU INTEND TO BECOME A UNITED STATES CITIZEN? <input type="checkbox"/> YES <input type="checkbox"/> NO					
14. ORGANIZATIONAL MEMBERSHIP					
LIST ALL ORGANIZATIONS EXCEPT LABOR UNIONS AND EXCEPT ORGANIZATIONS REFERRED TO IN ITEM 27 BELOW IN WHICH YOU HOLD OR HAVE HELD MEMBERSHIP. IF NONE, SO STATE.					
NAME AND ADDRESS		TYPE	OFFICE HELD	FROM (Date)	TO (Date)
15. MILITARY SERVICE					
a. COUNTRY	BRANCH OF SERVICE		SERVICE NUMBER	FROM (Date)	TO (Date)
b. ARE YOU A MEMBER OF A RESERVE COMPONENT? <input type="checkbox"/> YES <input type="checkbox"/> NO (If answer is "YES", furnish service, component and current status under Item 21, "Remarks".)					
c. LOCAL DRAFT BOARD (United States) AND ADDRESS				d. SELECTIVE SERVICE NO.	e. CLASSIFICATION

FURTHER INSTRUCTIONS: DO NOT COMPLETE PARTS III OR IV AT THIS TIME. Return this partially completed form to your employer who will review it to assure all entries are complete and the form is properly filled in. After return, proceed with completion of Parts III and IV.

PART III		
<p>Complete the items below in private. The answers or statements in this Part are privileged information between you and the Government. You should enter in Item 28 any information relating to your answers which might require further explanation, or any additional information which may have a bearing on your security clearance.</p>		
<p>22. HAVE YOU EVER BEEN ARRESTED, CHARGED, OR HELD BY ANY LAW ENFORCEMENT AUTHORITIES FOR ANY VIOLATION OF ANY LAW, REGULATION OR ORDINANCE? INCLUDE ALL COURTS-MARTIAL. DO NOT INCLUDE ANYTHING THAT HAPPENED BEFORE YOUR 16TH BIRTHDAY. DO NOT INCLUDE TRAFFIC VIOLATIONS FOR WHICH THE ONLY PENALTY IMPOSED WAS A FINE OF \$25.00 OR LESS. ALL OTHER CHARGES MUST BE INCLUDED EVEN IF THEY WERE DISMISSED.</p> <p><input type="checkbox"/> YES <input type="checkbox"/> NO IF "YES", GIVE DATE AND PLACE. CHARGE, AND DISPOSITION:</p>		
<p>23. WHAT TYPE OF DISCHARGE DID YOU RECEIVE, IF ANY, FROM MILITARY SERVICE?</p>		
<p>24. HAVE YOU EVER HAD A SECURITY CLEARANCE SUSPENDED, DENIED, OR REVOKED? (If answer is "YES", indicate level of clearance, when suspended, denied or revoked, by whom and where employed under Item 28, "Remarks". If you since have been granted a clearance by the government, indicate under Item 28, "Remarks", the date, level of clearance and activity which restored the clearance.)</p> <p><input type="checkbox"/> YES <input type="checkbox"/> NO</p>		
25.	YES	NO
<p>a. DO YOU HAVE A HISTORY OF MENTAL OR NERVOUS DISORDERS?</p>		
<p>b. ARE YOU NOW OR HAVE YOU EVER BEEN ADDICTED TO THE USE OF HABIT FORMING DRUGS SUCH AS NARCOTICS OR BARBITURATES?</p>		
<p>c. ARE YOU NOW OR HAVE YOU EVER BEEN A CHRONIC USER TO EXCESS OF ALCOHOLIC BEVERAGES?</p>		
<p>(If answer to any of the above is "YES", explain. Give names and addresses of hospitals, clinics, sanitariums, and physicians who have examined or treated you for such conditions.)</p>		
<p>26. AUTHORITY TO RELEASE MEDICAL INFORMATION</p> <p>I HEREBY GRANT PERMISSION TO THE DEPARTMENT OF DEFENSE TO OBTAIN AND REVIEW COPIES OF MY MEDICAL AND INSTITUTIONAL RECORDS RELATING TO CONDITIONS LISTED IN ITEM 25 AND TO QUESTION THOSE WHO HAVE EXAMINED OR TREATED ME THEREFOR.</p>		
SIGNATURE OF EMPLOYEE		DATE
<p>27. ORGANIZATIONAL MEMBERSHIP</p>		
<p>a. ARE YOU NOW, OR HAVE YOU EVER BEEN, A MEMBER OF THE COMMUNIST PARTY, U.S.A., THE COMMUNIST POLITICAL ASSOCIATION, THE YOUNG COMMUNIST LEAGUE, OR ANY COMMUNIST ORGANIZATION?</p>		
<p>b. ARE YOU NOW OR HAVE YOU EVER BEEN A MEMBER OF ANY FOREIGN OR DOMESTIC ORGANIZATION, ASSOCIATION, MOVEMENT, GROUP, OR COMBINATION OF PERSONS WHICH IS TOTALITARIAN, FASCIST, COMMUNISTIC, OR SUBVERSIVE, OR WHICH HAS ADOPTED, OR SHOWS, A POLICY OF ADVOCATING OR APPROVING THE COMMISSION OF ACTS OF FORCE OR VIOLENCE TO DENY OTHER PERSONS THEIR RIGHTS UNDER THE CONSTITUTION OF THE UNITED STATES OR WHICH SEEKS TO ALTER THE FORM OF GOVERNMENT OF THE UNITED STATES BY UNCONSTITUTIONAL MEANS?</p>		
<p>IF YOUR ANSWER TO EITHER OF THE ABOVE QUESTIONS IS "YES", LIST IN ITEM 28, THE NAMES OF ALL SUCH ORGANIZATIONS, ASSOCIATIONS, MOVEMENTS, GROUPS OR COMBINATION OF PERSONS AND DATES OF MEMBERSHIP. GIVE COMPLETE DETAILS OF YOUR ACTIVITIES THEREIN AND MAKE ANY EXPLANATION YOU DESIRE REGARDING YOUR MEMBERSHIP OR ACTIVITIES.</p>		
<p>28. REMARKS (Use the space provided below and attach additional sheets, if necessary.)</p>		
<p>(COMPLETE PART IV ON REVERSE SIDE OF ORIGINAL COPY)</p>		

PART IV		
<p>IMPORTANT NOTICE: Your signature on the following certification must be witnessed; the witness may be an employee of your firm. Prior to affixing your signature to the form, remove all carbons, fold the form so that the witness to your signature will not see any portion of Part III of the completed Personnel Security Questionnaire. Sign and date the form in the presence of the witness. Have the witness affix his signature and his address to the appropriate blocks on the form.</p>		
<p>NOTE: PENALTY FOR MISREPRESENTATION- Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false, or partial answers) may serve as a basis for denial of clearance for access to classified Department of Defense information. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of 5 years imprisonment, \$10,000 fine, or both, knowingly and willfully to make a false statement or representation to any Department or Agency of the United States as to any matter within the jurisdiction of any Department or Agency of the United States.</p> <p><i>This includes any statement knowingly and willfully made by employer or employee herein which is knowingly incorrect, incomplete or misleading in any important particular. Title 18 United States Code 911 states "whoever falsely and willfully represents himself to be a citizen of the United States shall be fined not more than \$1,000 or imprisoned not more than three years, or both".</i></p>		
<p align="center"><u>CERTIFICATION</u></p> <p>WARNING: Read every sentence of the Certification before signing. I certify that my above answers are true, complete, and correct to the best of my knowledge and belief, and are made in good faith. I certify that I know that any misrepresentation or false statement made by me herein may subject me to prosecution under Section 1001 of the United States Criminal Code, with penalties up to five (5) years imprisonment and \$10,000 fine, and provide a basis for denial of security clearance. I certify that I have read and understand each sentence of this Certification.</p>		
SIGNATURE OF WITNESS	SIGNATURE OF EMPLOYEE	DATE OF SIGNATURE
ADDRESS OF WITNESS (City, County, State)		
<p align="center"><u>INSTRUCTIONS TO EMPLOYEE UPON COMPLETION OF ABOVE</u></p> <p>Now that the form is signed and witnessed, place it in the pre-addressed envelope furnished (DSA Form 703), together with the completed FD Form 258 (Fingerprint Card), seal the envelope, sign across the envelope flap on the line provided, and affix the date of signature. Deliver the sealed envelope to your employer immediately.</p>		

F. Contract Security Classification Specification (DD Form 254)

1. The completed DD Form 254, attachments and supplements, as applicable, is the basic document by which classification, regrading and declassification specifications are documented and provided to prime and subcontractors. It is designed to indicate by a combination of a check list and narrative comment, the classified areas of information involved in the classified effort, and particularly to identify the specific items of information which require security classification protection. Responsibility for preparation of the prime contract DD Form 254 rests with the contracting officer or his designated representative of the User Agency concerned but the assistance of the contractor is encouraged. Based upon the classification guidance received, each contractor is responsible for developing the DD Form 254 for each classified subcontract, request for proposal or other solicitation let to subcontractor facilities. The contractor shall submit the recommended DD Forms 254 for each classified subcontract, other than service, graphic arts, research or commercial carrier subcontracts (see paragraph 60h) to the ACO for approval and distribution. When the prime contractor receives a revised DD Form 254 that does not require a related change in the subcontractor's DD Form 254, or receives written notice that annual review has resulted in no change in the existing specification, he shall reaffirm guidance to each subcontractor. The prime contractor does this by providing a true copy of the notice of reaffirmation received by the prime contractor or a true copy of pages 1 and 2 of the revised DD Form 254 received by the prime contractor annotated, "This revised DD Form 254 does not affect your current DD Form 254 dated". In either of these cases, ACO/PCO authentication is not required.

2. The DD Form 254 embodies the concept that the sensitive information itself shall be

identified and assigned a proper classification rather than assigning a classification to media by which classified information could be, or would likely be, conveyed. This method of classifying information rather than media is intended to identify most precisely the functional matter which is to be protected, thus providing, for example, the answer to the question of "What is there about a specific item of hardware which causes it to be classified?"

3. Whenever the prime contractor will be required to use classified GFE or GFP in the performance of the contract, the contracting officer or his representative shall inform the prime contractor what information requires protection by furnishing a DD Form 254 or other appropriate notification for each item of classified GFE or GFP to be used. The same procedure shall be followed in those instances where previously classified equipment is not Government furnished but where the prime contractor is authorized to purchase such classified equipment for use in the performance of his contract.

4. Items 1 through 14 and item 16 of the DD Form 254 provide the general administrative and contractual information pertaining to the classification specification of the classified effort. Item 15 of DD Form 254 and any supplements and attachments are used to provide the specified classification, downgrading and declassification information. Each item of the DD Form 254 is to be completed; N/A shall be shown for items which are not applicable. Classified information should not be entered on the DD Form 254. Classified information should be transmitted separately and appropriate reference entered in item 15 of the DD Form 254. The following numbered instructions correspond to the numbered items on the DD Form 254:

- a. 1. Insert highest level of clearance required for access to classified information in performance of the classified effort.

If the facility requires a clearance higher than the current clearance, the prime contractor may request the appropriate cognizant security office to upgrade the subcontractor's facility clearance.

- b. 2. Check item a., b., or c., as applicable.
- c. 3. In item 3a, enter the User Agency prime contract identification number. In addition, if this DD Form 254 is for a subcontract of the first tier, enter in item 3b the identification number of the first tier subcontract. For second tier and beyond subcontracts, enter in item 9a or 15, as applicable, the identification number and estimated date of completion or termination of the subcontract. If item 3c is used, enter appropriate data identifying the RFP, RFQ or IFB. If the solicitation is unclassified and the DD Form 254 is being used only to reflect access requirements of the contract/subcontract to be awarded, annotate item 11o "Remarks" to indicate that pre-award access is not required and the DD Form 254 indicates classification guidance for the contract/subcontract to be awarded. When re-issuing a currently valid subcontract DD Form 254 for a follow-on subcontract, indicate the new subcontract number in item 3b.
- d. 4. Furnish date for a, b., or c., as applicable.
- e. 5. Check item a., b., or c., as applicable and provide complete date. For item b., also show revision number.
- f. 6. Check "yes" or "no", as applicable. If "yes", complete items a., and b., and in item c., indicate whether accountability is or is not transferred.
- g. 7. If there is a prime contract, com-

plete items a., b., and c., to show the complete name, address and FSC number of the prime contractor's facility which will receive classified information in the performance of the prime contract listed in item 3a., and the cognizant security office of that facility. If there is no prime contract and item 3c is completed, enter instead in items a., b., and c., the name, address and FSC number of the contractor's facility to which this DD Form 254 is to be sent in connection with the FRP, RFQ, or IFB, and the cognizant security office of that facility.

- h. 8. If there is a first tier subcontract, complete items a., b., and c., to show the complete name, address, and FSC number of the subcontractor's facility which will receive classified information in performance of the subcontract listed in item 3b. If there is no first tier subcontract and item 3c is completed, enter instead the name, address, and FSC number of the subcontractor's facility to which this DD Form 254 is to be sent in connection with the RFP, RFQ, or IFB, and the cognizant security office of that facility.
- i. 9. If there is a second tier subcontract, complete items a., b., and c., to show the complete name, address and FSC number, and cognizant security office of the subcontractor's facility which will receive classified information in performance of the subcontract listed in item 3b. In item 9a., also provide the second tier subcontract number and estimated date of completion. If there is no second tier subcontract and item 3c is completed, enter instead the name, address and FSC number of the facility to which this DD Form 254 is to be sent in connection with the RFP, RFQ, or IFB, and the cog-

→ nizant security office of that facility. For subcontracting beyond the second tier, enter in item 15 or furnish on an attached sheet, the information specified above for that tier subcontractor and the cognizant security office of that facility.

→ j. 10. Under item a., provide a brief, yet sufficiently complete, unclassified statement to identify the nature of the procurement. If an unclassified statement cannot be made, enter the word "classified". Under item b., furnish the DoDAAD number of the Government procuring activity (identified in item 16d). For subcontracts the DoDAAD number will be that assigned the ACO. Where DD Forms 254 are approved by a contractor, item b will be annotated "N/A". Information pertaining to the DoDAAD number, six digits, is published in the DoD Activity Address Directory, DoD 4000.25-D, and a microfiche listing may be purchased from the GPO. The contractor may also contact his cognizant security office which has the listing. Under item c., check appropriate block to indicate whether or not contract prescribes security requirements which are additional to those described in the DD Form 441 and this Manual. If applicable, the User Agency shall furnish a copy of the special security requirements to the contractor, the ACO, if any, and the cognizant security office. Under item d., check appropriate box to indicate if any elements of the contract are outside the inspection responsibility of the cognizant security office. If Yes, explain in item 15 and identify specific areas or elements. However, discretion must be used in identifying other "specific areas or elements" so that disclosure restrictions are respected.

k. 11. Check appropriate box for each item listed. Use the "Remarks" block to elaborate as necessary.¹ If DDC or Defense Information Analysis Center services are requested, the DD Form 1540 and DD Form 1541 should be prepared and processed in accordance with component implementations of DoD Instruction 5200.21. Whenever possible, the DD Form 1540 should be prepared and forwarded simultaneously with the DD Form 254.

i. 12. In subcontracting situations, item b will contain the signature and typed name and title of the security supervisor of the facility issuing the subcontract. Inquiries pertaining to classification guidance, determinations or interpretations shall be directed to this official.

m. 13. Subcontractors of all tiers shall be instructed via item b., to submit proposed public releases through the prime contractor listed in item 7a., who will process the release in accordance with the guidance provided in the DD Form 254 for the prime contract.

n. 14. Read and closely observe the instructions presented at the top half of the item. Check applicable block(s) to indicate the manner in which the security classification guidance is conveyed for this classified effort. Classified narratives or guides shall always be transmitted under separate cover. When item b., is checked, list guide(s) under item 15 or in an attached list. When item c., is checked, enter in item

¹ The entry into a controlled area, per se, will not constitute access to classified information if the security measures which are in force prevent the gaining of knowledge of the classified information. Therefore, the entry into a controlled area under conditions that prevent the gaining of knowledge of classified information will not necessitate a personnel security clearance.

15 the appropriate instructions from paragraph 60h or paragraph 7-102d(4), ISR. (See paragraph 5 below for an explanation of commonly used terms.) Check item d., if this is a final DD Form 254 and item 6 has a "No" answer. Check item e., and provide date for review when annual review of DD Form 254 is required.

o. 15. To be used for remarks, as appropriate.

p. 16. The contracting officer or his authorized designee, after reviewing the DD Form 254 to insure adequacy, will affix his signature in item c., and items b., d., and e., will be completed to furnish appropriate identifying information concerning the approving official.

5. Narratives or classification guides used to provide the security classification specification and the downgrading/declassification instructions should clearly identify the specific details of information which warrant security protection against unauthorized disclosure. It is important to assure that statements of classification are clear enough to be easily understood and applied readily in determining which items of information in the contractual effort require a security classification. To assist the writer and user of the security classification specification, there are listed below several terms which are commonly used in the description of that information which may require classification, together with their generally accepted meanings. However, this does not preclude inclusion of terms devoted to a particular classified effort or an additional page(s) of the narrative/guide.

a. *Accuracy.* Precision with which the designed function is performed.

b. *Altitude.* The vertical distance of a level, a point, or an object considered as a

point, measured from mean sea level.

(1) Maximum—altitude beyond which performance is not possible.

(2) Minimum—altitude below which performance is not possible.

(3) Optimum—altitude spread at which performance is most satisfactory or effective.

c. *Blast Effect.* Destruction of or damage to structures and personnel by the force of an explosion on or above the surface of the ground. Blast effect may be contrasted with the cratering and groundshock effects of a projectile or charge which goes off beneath the surface.

d. *Circular Error Probability.* An indicator of the delivery accuracy of a weapon system, used as a factor in determining probable damage to a target. It is the radius of a circle within which half of the missiles/projectiles are expected to fall.

e. *Command and Control System.* The facilities, equipment communications, procedures, and personnel essential to a commander for planning, directing and controlling operations of assigned forces pursuant to the missions assigned.

f. *Counter-Countermeasures Capability.* Design features of the end item which are intended specifically to overcome enemy interference. (Electronic counter-countermeasures is that division of electronic warfare involving actions taken to insure friendly effective use of the electro-magnetic spectrum despite the enemy's use of electronic warfare. Electronic countermeasures is that division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electro-magnetic spectrum.)

g. *Depth.* The vertical distance from the plane of the hydrographic surface to a level,

a point, or an object considered as a point below the surface.

- (1) *Maximum*—depth below which performance is not possible.
- (2) *Minimum*—depth above which performance is not possible.
- (3) *Optimum*—depth spread at which performance is most satisfactory or effective.

→ *h. Design Information.* Technique, principle, or design feature, or the unique application thereof which in and of itself requires classification. The design information which requires protection must be specified.

→ *i. End Item.* A final combination of end products, component parts, and/or materials which is ready for its intended use, e.g., ship, tank, mobile machine shop, aircraft.

→ *j. Endurance.* The time an aircraft can continue flying or a ground vehicle or ship can continue operating under specified conditions, e.g., without refueling.

→ *k. Formula or Material.* Chemical or physical nature of the ingredient(s) and its proportions, of which all or part of the end item is composed.

→ *l. Fuel or Propellant.* Source of energy.
Type. Identification of fuel/propellant.

→ *m. Initial Operational Capability.* The first attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specific characteristics, and which is manned or operated by an adequately trained, equipped, and supported military unit or force.

→ *n. Lethality/Critical Effects.* The ability to cause a specified degree of damage to the target or to incapacitate personnel (including physical, physiological, and psychological effects).

o. Maneuverability. Ability to change position or direction. ←

p. Military Application. Use or purpose for which the end item is intended in sufficient detail that performance and/or tactical application is revealed or implied. ←

q. Military Characteristics. Those characteristics of equipment upon which depend its ability to perform desired military functions. Military characteristics include physical and operational characteristics but not technical characteristics. ←

r. Mission. The task, together with the purpose, which clearly indicates the action to be taken and the reason therefor. ←

s. Operational Characteristics. Those military characteristics which pertain primarily to the functions to be performed by equipment, either alone or in conjunction with other equipment, e.g., for electronic equipment, operational characteristics include such items as frequency coverage, channeling, type of modulation, and character of emission. ←

t. Operational Readiness (Alert) Time/Time Cycle. Sequence and duration of important operations to be performed on or by the end items or specified component thereof during a normal cycle of function such as emplacement, loading and firing/launching, warmup prior to operation, etc. ←

u. Orbit/Trajectory. Path of travel. ←

v. Range. The distance between any given point and an object or target. Also, the extent or distance limiting the operation or action of something such as the range of an aircraft, ship, or gun. ←

(1) *Maximum*—greatest distance attainable. ←

(2) *Minimum*—least distance attainable or allowable. ←

→ (3) *Optimum*—range spread at which performance is most satisfactory or effective.

→ *w. Reliability*. Probability that the design function will be performed at/for a specified time, and/or within specified limits.

→ *x. Resolutions*. Ability to analyze characteristics of a complex nature (such as signals, target signature characteristics, etc.) and to distinguish between them.

→ *y. Signature Characteristics*. Acoustic, magnetic, thermal, radiological, mechanical, electromagnetic, etc., phenomena which are critical to the operation of the end item or a component thereof, or which identify or reveal its presence.

→ *z. Speed/Velocity*. Rate of movement or motion.

→ (1) Maximum—greatest speed/velocity attainable.

→ (2) Cruising—speed/velocity at which greatest efficiency is attained.

→ (3) Takeoff or Launching—speed/velocity to initiate flight.

→ (4) Landing—speed/velocity in terminating flight.

(5) Acceleration and/or Deceleration—rate of change of speed/velocity.

aa. System Capability. Maximum number of operations which the end item can perform simultaneously in carrying out its design function.

ab. Technical Characteristics. Those characteristics of equipment which pertain primarily to the engineering principles involved in producing equipment possessing desired military characteristics, e.g., for electronic equipment, technical characteristics include such items as circuitry, and types and arrangement of components.

ac. Terminal Ballistics. Effects and action of a missile or projectile when it impacts or bursts at the target.

ad. Thrust. Impelling force delivered.

(1) Classes—maximum thrust expressed as an approximation or within a grouping.

(2) Specific—exact maximum thrust.

(3) Specific Impulse—amount of thrust in pounds that can be maintained for one second by one pound of fuel.

ae. Vulnerability. Susceptibility to defeat by the enemy.

DoD 5220.22-M

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: _____	
2. THIS SPECIFICATION IS FOR:		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts)	4. DATE TO BE COMPLETED (Estimated)
5. THIS SPECIFICATION IS: (See "NOTE" below. If item b or c is "X'd", also enter date for item a)			
a. PRIME CONTRACT	a. PRIME CONTRACT NUMBER	a. DATE	a. ORIGINAL (Complete date in all cases)
b. SUBCONTRACT (Use Item 15 for subcontracting beyond second tier)	b. FIRST TIER SUBCONTRACT NO.	b. DATE	b. REVISED (supersedes all previous specifications)
c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION	c. IDENTIFICATION NUMBER	c. DUE DATE	c. FINAL
6. Is this a follow-on contract? <input type="checkbox"/> Yes <input type="checkbox"/> No. If YES, complete the following:			
a. PRECEDING CONTRACT NUMBER		b. DATE COMPLETED	
c. Accountability for classified material on preceding contract			
<input type="checkbox"/> Is not, transferred to this follow-on contract.			
7a. Name, Address & Zip Code of Prime Contractor *		b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
8a. Name, Address & Zip Code of First Tier Subcontractor *		b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ *		b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
* When actual performance is at a location other than that specified, identify such other location in Item 15.			
10a. General identification of the Procurement for which this specification applies			b. DoDAAD Number of Procuring Activity identified in Item 16d.
c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? <input type="checkbox"/> Yes <input type="checkbox"/> No. If YES, identify the pertinent contractual documents in Item 15.			
d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? <input type="checkbox"/> Yes <input type="checkbox"/> No. If YES, explain in Item 15 and identify specific areas or elements.			
11. ACCESS REQUIREMENTS		YES	NO
a. Access to Classified Information Only at other contractor/Government activities.			
b. Receipt of classified documents or other material for reference only (no generation).			
c. Receipt and generation of classified documents or other material.			
d. Fabrication/Modification/Storage of classified hardware.			
e. Graphic arts services only.			
f. Access to IPO information.			
g. Access to RESTRICTED DATA.			
h. Access to classified COMSEC information.			
i. Cryptographic Access Authorization required.			
j. Access to SENSITIVE COMPARTMENTED INFORMATION.			
k. Access to other Special Access Program information (Specify in Item 15).			
l. Access to U. S. classified information outside the U. S., Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories.			
m. Defense Documentation Center or Defense Information Analysis Center Services may be requested.			
n. Classified ADP processing will be involved.			
o. REMARKS:			
12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (Item 16e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts).			
a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.			
b. Typed name, title and signature of program/project manager or other designated official		c. Activity name, address, Zip Code, telephone number and office symbol	
NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.			

DD FORM 254
1 JAN 78

EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE

<p>13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual (paragraph 5a and Appendix IX).</p>	
<p>b. Proposed public releases shall be submitted for approval prior to release <input type="checkbox"/> Direct <input type="checkbox"/> Through (Specify):</p>	
<p>to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) * for review in accordance with paragraph 5a of the Industrial Security Manual. * In the case of non-DoD User Agencies, see footnote, paragraph 5a, Industrial Security Manual.</p>	
<p>14. Security Classification Specifications for this solicitation/contract are identified below ("X" applicable box(es) and supply attachments as required). Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide: (I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading (if applicable). The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.</p>	
<p><input type="checkbox"/> a. A completed narrative is (1) <input type="checkbox"/> attached, or (2) <input type="checkbox"/> transmitted under separate cover and made a part of this specification. <input type="checkbox"/> b. The following classification guide(s) is made a part of this specification and is (1) <input type="checkbox"/> attached, or (2) <input type="checkbox"/> transmitted under separate cover. (List guides under Item 15 or in an attachment by title, reference number and date). <input type="checkbox"/> c. Service-type contract/subcontract. (Specify instructions in accordance with ISR/ISM, as appropriate.). <input type="checkbox"/> d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated _____ retention of the identified classified material is authorized for a period of _____. <input type="checkbox"/> e. Annual review of this DD Form 254 is required. If "X'd", provide date such review is due: _____.</p>	
<p>15. Remarks (Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions).</p>	
<p>16a. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in Item 16b below.</p>	
<p>REQUIRED DISTRIBUTION:</p> <p><input type="checkbox"/> Prime Contractor (Item 7a) <input type="checkbox"/> Cognizant Security Office (Item 7c) <input type="checkbox"/> Administrative Contracting Office (Item 16a) <input type="checkbox"/> Quality Assurance Representative <input type="checkbox"/> Subcontractor (Item 8a) <input type="checkbox"/> Cognizant Security Office (Item 8c) <input type="checkbox"/> Program/Project Manager (Item 12b) <input type="checkbox"/> U. S. Activity Responsible for Overseas Security Administration</p> <p>ADDITIONAL DISTRIBUTION: <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/></p>	<p>b. Typed name and title of approving official</p> <p>c. Signature</p> <p>d. Approving official's activity address and Zip Code</p> <p>e. Name, address and Zip Code of Administrative Contracting Office</p>

H. Applicant Fingerprint Card (FD Form 258)

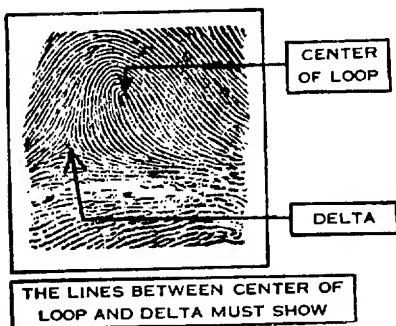
→ This form is completed for all personnel being considered for a personnel security clearance, a Canadian Reciprocal Clearance, or a U.K. Reciprocal Clearance by DISCO. Completion of the form is a prerequisite to

the granting of such actions. Care shall be exercised to insure that fingerprints are authentic, legible, and complete, as forms which do not meet prescribed standards shall be returned for re-execution which will result in clearance delays.

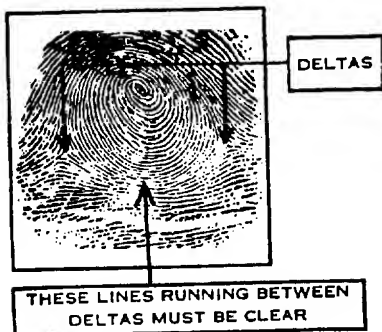
**FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
WASHINGTON, D.C. 20537**

APPLICANT

1. LOOP



2. WHORL



3. ARCH



To obtain classifiable fingerprints:

1. Use printer's ink.
2. Distribute ink evenly on inking slab.
3. Wash and dry fingers thoroughly.
4. Roll fingers from nail to nail, and avoid allowing fingers to slip.
5. Be sure impressions are recorded in correct order.
6. If an amputation or deformity makes it impossible to print a finger, make a notation to that effect in the individual finger block.
7. If some physical condition makes it impossible to obtain perfect impressions, submit the best that can be obtained with a memo stapled to the card explaining the circumstances.
8. Examine the completed prints to see if they can be classified, bearing in mind that most fingerprints fall into the patterns shown on this card (other patterns occur infrequently and are not shown here).

This card for use by:

LEAVE THIS SPACE BLANK

1. Law enforcement agencies in fingerprinting applicants for law enforcement positions and applicants for licenses or permits required by local ordinance or official regulation. The reason for fingerprinting must be shown in appropriate block. A set of applicant prints must first be checked through state identification bureau before submission is made to FBI (through local bureau where there is no state central bureau). Only those fingerprints for which no record has been found locally should be submitted for FBI search. Place notation in upper right-hand corner on this side of fingerprint card to show check made. If a more current copy of an existing FBI identification record is required, simply supply name, FBI number or local arrest number and, if readily available, the primary and secondary parts of the fingerprint classification.

2. U.S. Government agencies in connection with clearances. Identity of private contractor should be shown in space "Company and Address." The contributor is the name of agency submitting the fingerprint card to the FBI.

FBI number, if known, should always be furnished in appropriate space.

I. REQUEST FOR VISIT OR ACCESS APPROVAL
(ERDA FORM 277)

This form is included for information pur-

poses. It is used for processing visits involving access to RESTRICTED DATA. Copies of this form may be obtained from the ERDA.

FORM ERDA-277
(6-76)
ERDAM 2501
Previous editions may be used.

U.S. ENERGY RESEARCH AND DEVELOPMENT ADMINISTRATION
REQUEST FOR VISIT OR ACCESS APPROVAL
(Not to be used for temporary or permanent personnel assignments.)

PART "A"

Date: _____
Prepared by: _____
Symbol: _____
Telephone No.—Commercial: _____ FTS: _____

Insert the office and address of ERDA Manager having operational control over the installation to be visited.
To: _____
From: _____

Insert contracting activity and address of User Agency supporting the visit request.
Enter the full name of each proposed visitor and his Social Security number.

State the purpose of the visit in sufficient detail to enable the addressee to ascertain the subject area involved, and to determine the level and scope of access required. Classified information will not be disclosed in this item.

It is requested that the following person(s) be granted visit/access approval:

LAST NAME, FIRST, MIDDLE INITIAL AND SOCIAL SECURITY NUMBER	CHECK		DATE OF BIRTH	ORGANIZATION	TYPE OF CLEARANCE	CLEARANCE NO.	DATE OF CLEARANCE
	U. S. CITIZEN	ALIEN					

NAME OF FACILITY (IES) TO BE VISITED: _____ FOR THE INCLUSIVE DATES: _____

FOR THE PURPOSE OF: _____

TO CONFER WITH THE FOLLOWING PERSON (S): _____

SPECIFIC INFORMATION TO WHICH ACCESS IS REQUESTED: _____

Prior arrangements have/have not been made as follows: _____

Access requested to:
Restricted Data ☐ Yes ☐ No
Other classified info ☐ Yes ☐ No

CERTIFICATION FOR PERSONNEL HAVING DOD CLEARANCE
This certifies that the person(s) named above needs this access in the performance of duty and that permitting the above access will not endanger the common defense and security.

Name and Title, Requesting DOD Official: _____

Title, Authorizing DOD Official (See DOD Directive 5210.2 and 5210.8): _____

Authorized access to Critical Nuclear Weapon Design Information (CNWDI) in Accordance with DOD Directive Executive Order 5210.2 ☐ Yes ☐ No

Signature (See AR 380-150; OPNAV 5310.3F; AFR 205-1): _____

CERTIFICATION FOR PERSONNEL HAVING ERDA CLEARANCE
This certifies that the person(s) named above needs this access in the performance of duty.

Title: _____

Requesting ERDA or Other Government Agencies: _____

PART "B"

Approval is granted with limitations indicated below: _____

Manager of Operations or Headquarters Division Director: _____

Insert the date on which the form is prepared.

Enter symbol and telephone number of contracting officer of activity identified in "From" line.

Federal telephone system.

Name and address of contractor facility.

For each proposed visitor, show the current highest level of access he is authorized, and the date of its issuance. For contractor personnel, use the date of the current letter of Consent (DISCO Form 560-R), which can be obtained from the contractor or from his cognizant security office. To be certified by the facility security supervisor.

Leave blank; this space is for use by the activity to be visited.

PRIVACY ACT INFORMATION STATEMENT

Collection of the information requested is authorized by Section 145 of the Atomic Energy Act of 1954, as amended (PL 83-703, 42 USC 2165). Compliance with this request is voluntary; however, if the information submitted is inadequate or incomplete, approval for your visit to a classified ERDA facility, or your access to classified information may be delayed or withheld. The information you furnish will be used by ERDA and ERDA contractors to control access to classified information and areas.

The Social Security number is not required for these purposes, but you may voluntarily furnish it to assist us in correct identification.

**J. Letter of Notification of Facility
Security Clearance
(DLA Form 381-R)**

This letter is used by the DCASR to notify
a facility that it has been granted a facility

security clearance. Letters of notification
shall not be duplicated, and the fact that a
facility security clearance has been granted
shall not be used for promotional or advertis-
ing purposes.

(Appropriate DCASR Letterhead)

Name and Address of Facility

Gentlemen:

Reference is made in our earlier correspondence regarding the eligibility of your facility for a Department of Defense security clearance. I am pleased to advise that the necessary processing has been completed and security clearance at the level is hereby granted your facility.

The fact that your organization has qualified for and been granted a facility security clearance may not be used for advertising or promotional purposes, nor may this letter be reproduced in any form except for the necessary records of your organization.

As your cognizant security office, we are vitally interested in assisting you in the development of a sound security posture. We will conduct periodic reviews of your program to aid you in maintaining proper security safeguards, and are available at any time for guidance or assistance.

Sincerely,

(Signature and Title)

DLA Form 381-R LETTER OF NOTIFICATION OF FACILITY SECURITY CLEARANCE
Oct 77

Edition of Dec 75
is obsolete

K. Letter of Notification of Security Assurance to a Foreign Government or International Pact Organization (DISCO Form 382)

The DISCO Form 382 is issued by DISCO, to provide Security Assurance concerning a

U.S. citizen who is employed by a cleared contractor and to whom the foreign activity desires to release its own classified information.¹

¹ If access to NATO classified information only is required for U.S. citizens employed by foreign contractors in NATO countries, consult the cognizant security office for procedural guidance.

(Appropriate DISCO Letterhead)

IN REPLY
REFER TO DISCO-C
SUBJECT:

SSAN:
DPOB:
FSCM:

YOUR REQUEST FOR A SECURITY ASSURANCE HAS BEEN PROCESSED. BASED ON THE EVALUATION OF THE PRESCRIBED INVESTIGATION, THE DEPARTMENT OF DEFENSE HEREBY ISSUES THE ABOVE NAMED INDIVIDUAL THE REQUESTED SECURITY ASSURANCE. REQUEST THIS LETTER BE RETURNED TO DISCO WHEN NO LONGER REQUIRED.

BY DIRECTION OF THE SECRETARY OF DEFENSE:

(Signature and Title)

DISCO Form 382
LETTER OF NOTIFICATION OF SECURITY ASSURANCE TO A FOREIGN GOVERNMENT OR INTERNATIONAL PACT ORGANIZATION

L. Department of Defense Security Agreement (DD Form 441) and Appendage (DD Form 441-1)

This form is used to obtain the formal agreement of management of a facility to abide by the DoD "Industrial Security Manual for Safeguarding Classified Information" (Attachment to DD Form 441). Once executed, a DD Form 441 continues in effect until terminated by one of the parties thereto, as provided for in Section IV, "Termination," of the form. Execution of the DD Form 441 is a prerequisite to processing of a facility security clearance. An appendage (DD Form 441-1), to be used when management desires to indicate multiple-facility coverage

with one Security Agreement, is included herewith. After a Security Agreement has been properly executed, a contractor may use the DD Form 441-1 to accomplish additions, deletions, or changes in the branches and/or facilities included in and covered by the DD Form 441. After the home office of a multiple facility organization has executed the DD Form 441, it is permissible for one of the executive personnel at the specific operating location of the company, including the facility security supervisor, to sign the DD Form 441-1. This authority may be exercised by the local management official provided he has the delegated authorization to do so, whether or not he is also an officer of the company.

DEPARTMENT OF DEFENSE
SECURITY AGREEMENT

THIS AGREEMENT, entered into this _____ day of _____ 19____

by and between THE UNITED STATES OF AMERICA through the Defense Contract Administration Services,
Defense Supply Agency
acting for the Department of Defense (*hereinafter called the Government*) and (i)

a corporation organized and existing under the laws of the State of _____

(ii) a partnership consisting of _____

(iii) an individual trading as _____

with its principal office and place of business at _____ in the city of _____

State of _____ (*hereinafter called the Contractor*).

WITNESSETH THAT:

WHEREAS, the Government, through the Department of the Army, the Department of the Navy, and/or the Department of the Air Force, has in the past purchased or may in the future purchase from the Contractor supplies or services which are required and necessary to the national defense of the United States; or may invite bids or request quotations on proposed contracts for the purchase of supplies or services which are required and necessary to the national defense of the United States; and

WHEREAS, it is essential that certain security measures be taken by the Contractor prior to and after his being accorded access to classified information; and

WHEREAS, the parties desire to define and set forth the precautions and specific safeguards to be taken by the Contractor and the Government in order to preserve and maintain the security of the United States through the prevention of improper disclosure of classified information derived from matters affecting the national defense; sabotage; or any other act detrimental to the security of the United States:

NOW, THEREFORE, in consideration of the foregoing and of the mutual promises herein contained, the parties hereto agree as follows:

Section I—SECURITY CONTROLS

(A) The Contractor agrees to provide and maintain a system of security controls within its or his own organization in accordance with the requirements of the Department of Defense Industrial Security Manual for Safeguarding Classified Information attached hereto and made a part of this agreement, subject, however, (i) to any revisions of the Manual required by the demands of national security as determined by the Government, notice of which has been furnished to the Contractor, and (ii) to mutual agreements entered into by the parties in order to adapt the Manual to the Contractor's business and necessary procedures thereunder. In order to place in effect such security controls, the Contractor further agrees to prepare *Standard Practice Procedures* for its or his own use, such procedures to be consistent with the Department of Defense Industrial Security Manual for Safeguarding Classified Information. In the event of any inconsistency between the Contractor's *Standard Practice Procedures* and the Department of Defense Industrial Security Manual for Safeguarding Classified Information as the same may be revised, the Manual shall control.

(B) The Government agrees that it shall indicate when necessary by security classification (*Top Secret, Secret, or Confidential*), the degree of importance to the national defense of information pertaining to supplies, services, and other matters to be furnished by the Contractor to the Government or the Government to the Contractor, and the Government shall give written notice of such security classification to the Contractor and of any subsequent changes thereof; provided, however, that matters requiring security classification will be assigned the least restrictive security classification consistent with proper safeguarding of the matter concerned, since overclassification causes unnecessary operational delays and depreciates the importance of correctly classified matter. Further, the Government agrees that when Atomic Energy information is involved it will when necessary indicate by a marking additional to the classification marking that the information is "Restricted Data—Atomic Energy Act, 1946." The Contractor is authorized to rely on any letter or other written instrument signed by the contracting officer changing the classification of matter. The Government also agrees upon written application of the Contractor to designate employees of the Contractor who may have access to information classified Top Secret or Secret or to information classified Confidential when "Restricted Data" is involved, or to matter involving research, development, or production of cryptographic equipment, regardless of its military classification; and alien employees to have access to any classified matter.

(C) The Contractor agrees that it or he shall determine that any subcontractor, subbidder, individual, or organization proposed by it or him for the furnishing of supplies or services which will involve access to classified information in its or his custody has executed a Department of Defense Security Agreement which is still in effect, with any Military Department, prior to being accorded access to such classified information.

Section II—INSPECTION

Designated representatives of the Government responsible for inspection pertaining to industrial plant security shall have the right to inspect at reasonable intervals the procedures, methods, and facilities utilized by the Contractor in complying with the requirements of the terms and conditions of the Department of Defense Industrial Security Manual for Safeguarding Classified Information. Should the Government, through its authorized representative, determine that the Contractor's security methods, procedures, or facilities do not comply with such requirements, it shall submit a written report to the Contractor advising him of the deficiencies.

Section III—MODIFICATION

Modification of this security agreement (as distinguished from the Industrial Security Manual for Safeguarding Classified Information, which may be modified in accordance with section I of this agreement) may be made only by written agreement of the parties hereto.

Section IV—TERMINATION

This agreement shall remain in effect until terminated through the giving of 30 days' written notice to the other party of intention to terminate; provided, however, notwithstanding any such termination, the terms and conditions of this agreement shall continue in effect so long as the Contractor has classified information in his possession or under his control.

Section V—PRIOR SECURITY AGREEMENTS

As of the date hereof, this security agreement replaces and succeeds any and all prior security or secrecy agreements, understand-

ings, and representations with respect to the subject matter included herein, entered into between the Contractor and the Department of the Army, the Department of the Navy, and/or the Department of the Air Force: *Provided*, That the term "security or secrecy agreements, understandings, and representations" shall not include agreements, understandings, and representations contained in contracts for the furnishing of supplies or services to the Government heretofore entered into between the Contractor and the Department of the Army, the Department of the Navy, and/or the Department of the Air Force.

Section VI—SECURITY COSTS

This agreement does not obligate Government funds, and the Government shall not be liable for any costs or claims of the Contractor arising out of this agreement or instructions issued hereunder. It is recognized, however, that the parties may provide in other written contracts for security costs which may be properly chargeable thereto.

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the day and year first above written:

THE UNITED STATES OF AMERICA

By _____

(Authorized representative of the Government)

(Corporation)

WITNESS

By _____

(Firm)

(Title)

(Address)

NOTE.—In case of corporation, witnesses not required but certificate below must be completed. Type or print names under all signatures.

NOTE.—Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the agreement and the certificate.

CERTIFICATE

I, _____, certify that I am the _____ of the corporation named as Contractor herein; that who signed this agreement on behalf of the Contractor, was then of said corporation; that said agreement was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.

(Corporate Seal)

(Signature)

APPENDAGE TO DEPARTMENT OF DEFENSE SECURITY AGREEMENT

It is further agreed, on this _____ day of _____, 19____, by and between the United States of America through the Defense Contract Administration Services, Defense Supply Agency, acting for the Department of Defense, hereinafter called the Government, and _____,

which has entered into the Security Agreement to which this appendix is made a part that the branches and/or facilities listed below, owned and/or operated by said contractor are included in and covered by the provisions of the said Security Agreement, and Certificate Pertaining to Foreign Affiliation, DD Form 441s.

the said Security Agreement, and Certificate Relating to Foreign Investment Act, 1950, and		
NAME OF PLANT OR FACILITY	NUMBER AND STREET ADDRESS	CITY AND STATE
THE UNITED STATES OF AMERICA		CONTRACTOR
BY		BY(Authorized Representative of Contractor)
AUTHORIZED REPRESENTATIVE OF THE GOVERNMENT		TITLE
		ADDRESS

This form is used to provide formal certification from the contractor relative to FOCI in order that the DoD may determine eligibility for a facility security clearance. In completing the DD Form 441s all items are to be answered by indicating "X" in either the "Yes" or "No" column. If an answer to any question is "Yes" the following paragraphs provide instructions for the submission of necessary data.

Question 1 - Identify the percentage of any class of shares or other securities issued which are owned by foreign interests, broken down by country. If you answer "Yes" and have received from an investor a copy of Schedule 13 D filed by the investor with the Securities and Exchange Commission, you are to attach a copy of Schedule 13 D to the revised DD Form 441s.

Question 2 - Furnish the name, address by country, and the percentage owned. Include name and title of officials of your facility who occupy positions with the foreign entity, if any.

Question 3 - Furnish full information concerning the identity of the foreign interest and the position he holds in your organization.

Question 4 - Identify the foreign interest(s) and furnish full details concerning the control or influence.

Question 5 - Furnish name of foreign interest, country, nature of agreement or involvement. Agreements include licensing, sales, patent exchange, trade secrets, agency, cartel, partnership, joint venture, proxy, etc. If you answer "Yes" and have received from the investor a copy of Schedule 13 D filed by the investor with the Securities and Exchange Commission, you are to attach a copy

Question 6 - Furnish the amount of indebtedness and by whom furnished as related to the current assets of the organization. Include specifics as to the type of indebtedness and what, if any, collateral, including voting stock, has been furnished or pledged. If any debentures are convertible, specifics are to be furnished.

Question 7 - State full particulars in respect to any income from Communist countries, including percentage from each such country as related to total income, and the type of services or products involved. If income is from non-Communist countries, give overall percentage as related to total income and type of services or products in general terms. If income is from a number of foreign countries, identify countries. Include also percentage by country.

Question 8 - Identify the institutional investors by name and address, include the percentage of voting stock held. If you answer "Yes" and have received from the investor a copy of Schedule 13 D filed by the investor with the Securities and Exchange Commission, you are to attach a copy of Schedule 13 D to the revised DD Form 441s.

Question 9 - Include identifying data on all such directors. If they have a security clearance, so state. Also indicate the name and address of all other corporations with which they serve in any capacity.

Question 10 - Provide complete information by identifying the individuals and the country of which they are a citizen. Category 4 (see paragraph 41d) visits are not included in the purview of this question.

Question 11 - Describe the foreign involvement in detail, including why the involvement would not be reportable in the preceding questions.

CERTIFICATE PERTAINING TO FOREIGN INTERESTS		TYPE OR PRINT ALL ANSWERS	Form Approved OMB No. 22-R0193
PENALTY NOTICE			
<p>PENALTY — Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false or partial answers) may serve as a basis for denial of clearance for access to classified Department of Defense information. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of five (5) years imprisonment, \$10,000 fine, or both, knowingly to make a false statement or representation to any Department or Agency of the United States, as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly incorrect, incomplete or misleading in any important particular.</p>			
PROVISIONS			
<p>1. This report is authorized by the Secretary of Defense pursuant to authority granted him by E.O. 10865. While you are not required to respond, your eligibility for a facility security clearance cannot be determined if you do not complete this form. The retention of a facility security clearance is contingent upon your compliance with the requirements of DoD 5220.22-M for submission of a revised form as appropriate.</p> <p>2. When this report is submitted in confidence and is so marked, applicable exemptions to the Freedom of Information Act will be invoked to withhold it from public disclosure.</p> <p>3. Complete all questions on this form. Answer each question in either the "Yes" or "No" column. If your answer is "Yes" furnish in full the complete information under "Remarks".</p>			
QUESTION		YES	NO
1. Do foreign interests own or have beneficial ownership in 5% or more of your organization's securities?			
2. Does your organization own any foreign interest in whole or in part?			
3. Do any foreign interests have positions, such as directors, officers, or executive personnel in your organization?			
4. Does any foreign interest control or influence, or is any foreign interest in a position to control or influence the election, appointment, or tenure of any of your directors, officers, or executive personnel?			
5. Does your organization have any contracts, agreements, understandings or arrangements with a foreign interest(s)?			
6. Is your organization indebted to foreign interests?			
7. Does your organization derive any income from Communist countries or income in excess of 10% of gross income from non-Communist foreign interests?			
8. Is 5% or more of any class of your organization's securities held in "nominee shares," in "street names" or in some other method which does not disclose the beneficial owner of equitable title?			
9. Does your organization have interlocking directors with foreign interests?			
10. Are there any citizens of foreign countries employed by or who may visit your facility (or facilities) in a capacity which may permit them to have access to classified information (exclude cleared immigrant aliens in answering this question)?			
11. Does your organization have any foreign involvement not otherwise covered in your answers to the above questions?			

DD FORM 441s
1 SEP 76

EDITION OF 1 MAR 60 IS OBSOLETE

REMARKS (Attach additional sheets, if necessary, for a full detailed statement)	
CERTIFICATION	
I CERTIFY that the entries made by me above are true, complete, and correct to the best of my knowledge and belief and are made in good faith.	
WITNESS:	
_____ _____ _____	_____ DATE CERTIFIED By _____ _____ CONTRACTOR _____ TITLE _____ ADDRESS
NOTE: In case of corporation, witnesses not required but certificate below must be completed. Type or print names under all signatures.	
NOTE: Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the agreement and the certificate.	
CERTIFICATE	
I, _____ certify that I am the _____ of the corporation named as Contractor herein; that _____ who signed this certificate on behalf of the Contractor, was then _____ of said corporation; that said certificate was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.	
(Corporate Seal)	_____ SIGNATURE AND DATE

**N. Security Briefing and Termination
Statements (Industrial Personnel)
(DLA Form 482)**

This is a two-part form prescribed for use by employees of contractors. Part I shall be executed by the employee following his initial security briefing and prior to being granted access to classified information, to certify that he has read and is familiar with the provisions of the Espionage Laws and other Federal criminal statutes applicable to the safeguarding of classified information. Part

II shall be executed by the employee during termination proceedings to make a like declaration. The use of this form shall supersede all local forms presently used by contractors.

The Espionage Laws and other Federal criminal statutes referred to in this form are the following sections of Title 18 of the United States Code: §§ 793, 794, 795, 796, 797, 798, 799, 2153, 2154, 2155, 2156, 371, and 797 of Title 50 United States Code. These sections of the United States Code are set forth in Appendix VI.

SECURITY BRIEFING AND TERMINATION STATEMENTS (INDUSTRIAL PERSONNEL)		
<p>Section 1001 of Title 18, United States Code, makes it a criminal offense, punishable by a maximum of five (5) years imprisonment, \$10,000 fine, or both, knowingly and willfully to make a false statement or representation to any Department or Agency of the United States, as to any matter within the jurisdiction of any Department or Agency of the United States.</p>		
<p><i>INSTRUCTION: Part I of this form shall be executed by an employee of a contractor following his initial security briefing, and prior to being permitted access to classified information. An employee who executes Part I and who subsequently is absent from place of employment, for any reason, for more than one year, must reexecute a new Part I before again being permitted access to classified information.</i></p>		
<p><i>Part II shall be executed by the employee:</i></p> <ul style="list-style-type: none"> <i>a. at the time of termination of employment (discharge, resignation, or retirement).</i> <i>b. at the beginning of a layoff or leave of absence for an indefinite period, or a prescribed period in excess of one year.</i> <i>c. if the employee's personnel security clearance is administratively terminated.</i> <i>d. if the employee's personnel security clearance is suspended or revoked by the Department of Defense.</i> <i>e. upon termination of the facility's security clearance.</i> <p><i>If the employee refuses to sign either part of this form, the contractor shall notify his cognizant security office immediately.</i></p>		
TYPED NAME OF EMPLOYEE (Last, First, Middle)		TYPED NAME OF CONTRACTOR
PART I - INITIAL SECURITY BRIEFING STATEMENT		
DATE OF BRIEFING	TYPED NAME AND TITLE OF PERSON BRIEFING EMPLOYEE	
<p>I hereby certify that I have received a security briefing. I shall not knowingly and willfully communicate, deliver, or transmit, in any manner, classified information to an unauthorized person or agency. I am informed that such improper disclosure may be punishable under Federal criminal statutes. I have been instructed in the importance of classified information, and in the procedure governing its safeguarding. I am informed that willful violation or disregard of security regulations may cause the loss of my security clearance. I have read, or have had read to me, the portions of the Espionage Laws and other Federal criminal statutes relating to the safeguarding of classified information reproduced in Appendix VI, "Department of Defense Industrial Security Manual." I will report to the Federal Bureau of Investigation and to my employer, without delay, any incident which I believe to constitute an attempt to solicit classified information by an unauthorized person.</p>		
TYPED NAME AND SIGNATURE OF WITNESS	DATE SIGNED	SIGNATURE OF EMPLOYEE
PART II - SECURITY TERMINATION STATEMENT		
<p>I certify that I have read, or have had read to me, the portions of the Espionage Laws and other Federal criminal statutes applicable to the safeguarding of classified information reproduced in Appendix VI, "Department of Defense Industrial Security Manual"; that I have surrendered all classified information in my custody; that I will not knowingly and willfully communicate, deliver or transmit, in any manner, classified information to an unauthorized person or agency; that I will report to the Federal Bureau of Investigation, without delay, any incident which I believe to constitute an attempt to solicit classified information by an unauthorized person; and that I (have) (have not) (<i>strike out inappropriate word or words</i>) also received a terminal, oral security briefing.</p>		
TYPED NAME AND SIGNATURE OF WITNESS	DATE SIGNED	SIGNATURE OF EMPLOYEE

O. Letter of Consent (DISCO Form 560)

The Letter of Consent is used by DISCO to notify a facility that one of its employees is authorized to have access to classified information of the category indicated. Letters of

Consent are not issued to individuals, therefore, this form shall not be released to employees. This form replaces DLA Form 560-R. DLA Forms 560-R previously issued remain valid until such time as they are superseded or terminated in accordance with the provisions of this Manual.

LAST NAME - FIRST NAME - MIDDLE				DATE	OTHER NAMES
SOCIAL SECURITY NO.		PLACE OF BIRTH			
DATE OF BIRTH	ODEP	PHYS LOC	CITIZEN OF		
LEVEL OF CLEARANCE					
NAME AND ADDRESS OF CONTRACTOR					
<p>GENTLEMEN: The consent of the Secretary of Defense is hereby granted for the above-named employee to have access to classified information up to and including the level shown, provided access is essential in connection with the performance of a classified contract. Unless suspended or revoked by the Department of Defense, or administratively terminated when access no longer is required, this personnel security clearance is valid as long as the individual is continuously employed by your organization. If this clearance is administratively terminated and a need for access develops later, or if employment is terminated and the individual is subsequently reemployed and requires access, this clearance may be reinstated provided not more than one year has elapsed since it was last valid. This consent will continue in effect if the employee is transferred to another facility of your organization if continued clearance is required, and provided DISCO is promptly notified. You are required to report promptly to DISCO any information coming to your attention which may indicate that continued access to classified information may not be clearly consistent with the national interest. A copy of this form shall not be furnished to the above-named employee for any purpose whatsoever. You may reproduce it only as necessary for your organization's essential records or to meet Department of Defense requirements. This form shall be returned to DISCO upon death of the employee, or whenever return is requested by the Government.</p>					
ISSUED BY Defense Industrial Security Clearance Office Columbus, Ohio				SIGNATURE OF AUTHORIZED REPRESENTATIVE	
<p align="center">LETTER OF CONSENT DEPARTMENT OF DEFENSE INDUSTRIAL SECURITY PROGRAM</p>					

DISCO FM 560 1 MAR 75
REPLACES DSA FM 560-R AND DISCO FM 561 (TEST) WHICH ARE OBSOLETE

**P. Request for and Certificate of
Cryptographic Access Authorization
(DD Form 560-3)**

use by contractors and their employees. It shall be executed in accordance with Section III, paragraphs 15 and 16. COMSEC Supplement to this Manual.

This is a four-part form prescribed for

DoD 5220.22-M

REQUEST FOR AND CERTIFICATE OF CRYPTOGRAPHIC ACCESS AUTHORIZATION			
PART I - REQUEST FOR ISSUANCE OF CRYPTOGRAPHIC ACCESS AUTHORIZATION (To Be Completed By Employer)			
TO: Defense Industrial Security Clearance Office Defense Supply Agency Columbus, Ohio 43215		FROM: (Name and Address of Employer)	
NAME OF EMPLOYEE	DATE OF BIRTH	PLACE OF BIRTH (City, County, and State)	
JOB TITLE AND DESCRIPTION OF EMPLOYEE'S DUTIES WHICH REQUIRE ACCESS TO CLASSIFIED INFORMATION			
CONTRACT NUMBER, IF ANY	SECURITY CLASSIFICATION OF CRYPTOGRAPHIC INFORMATION TO WHICH EMPLOYEE WILL REQUIRE ACCESS	EXISTING SECURITY CLEARANCE	
TYPED NAME OF EMPLOYER OR DESIGNATED REPRESENTATIVE	SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE	DATE	
PART II - CRYPTOGRAPHIC ACCESS AUTHORIZATION (To Be Completed By U. S. Government)			
_____ (Name of Employee) employed by _____ (Contractor) is authorized access to cryptographic information classified no higher than _____ (Classification). He (is) (is not) authorized access to operational U. S. Government traffic incident to installation, maintenance or operation of cryptographic equipment for the Government.			
TYPED NAME OF ORGANIZATION	SIGNATURE OF AUTHORIZING OFFICIAL	DATE	
PART III - BRIEFING CERTIFICATE (To Be Completed By Employee)			
I, _____ hereby certify that I have received a briefing on cryptographic security from _____ on _____ 19____. I understand fully the information presented at the briefing and am aware that any willful disclosure of classified cryptographic information to unauthorized persons will make me subject to prosecution under the criminal laws of the United States. I understand that any COMSEC system equipment, development, study or proposal which I may originate after having access to cryptographic information must be submitted to the contracting officer or the Assistant Director, National Security Agency for evaluation. I understand that the safeguarding of cryptographic information is of the utmost importance, and that the loss or compromise of this information could lead to irreparable damage to the United States. I have been instructed in the general nature of cryptographic material and the general principles of its protection. I have carefully read the pertinent regulations which govern the handling and safeguarding of that cryptographic information to which I am being granted access, and I am familiar with the provisions of Sections 793, 794 and 798, Title 18, U. S. Code.			
SIGNATURE OF WITNESS	SIGNATURE OF EMPLOYEE	DATE	
PART IV - DEBRIEFING CERTIFICATE (To Be Completed By Employee)			
I, _____ certify that I have received a debriefing from _____ on _____ 19____ and I understand the importance to the national security of continuing to safeguard cryptographic information. I also understand that I am still bound by all security regulations pertaining to classified cryptographic information and that I am subject to criminal penalties prescribed by law for its willful disclosure to unauthorized persons.			
SIGNATURE OF WITNESS	SIGNATURE OF EMPLOYEE	DATE	

DD FORM 560-3
1 DEC 65

REPLACES EDITION OF 1 OCT 64 WHICH IS OBSOLETE

GPO 826-330

Q. Personnel Security Clearance Change Notification (DLA Form 562-R)

a. This is a multi-purpose form used by the contractor to report one of the following occurrences concerning a cleared employee or an employee for whom a clearance has been requested. The forms are submitted to DISCO except when the individual concerned is cleared or in the process of being cleared in connection with the facility security clearance as required by paragraph 22, in which case the forms shall be submitted to the cognizant security office. The cognizant security office, after annotating its own records will forward the forms to DISCO. In the case of a termination or change of name only one copy is required; in the case of a multiple facility transfer, reinstatement of clearance, downgrading of a TOP SECRET clearance or reinstatement of a previously downgraded TOP SECRET clearance, an original and one copy are required. In the latter four situations, DISCO will annotate the copy of the form, acknowledging its receipt and return it to the contractor. In the case of a change of name, DISCO will issue a new Letter of Consent. When requesting reinstatement of a clearance, downgrading of a TOP SECRET clearance, or reinstatement of a previously downgraded TOP SECRET clearance, the name and address of the submitting facility shall appear in the "Remarks" and "Return To" portions of the form. In the case of a multiple facility transfer, the name and address of the facility to which the individual is transferred shall be included in the "Remarks" block; the name and address of the submitting facility shall appear in the "Return To" portion of the form.

b. The form shall be used by the contractor to report the following:

- (1) Clearance transfers within a multiple facility organization (see paragraph 26f). The name and address of the facility to which the individual is transferred shall be included in the "Remarks" block of the form.

- (2) Reemployment of cleared personnel (see paragraph 26h). Indicate "Reemployment (date)" in the "Remarks" block of the form.

- (3) Change of Name (paragraph 26j). The name of the individual exactly as shown on the Letter of Consent (or on the DD Form 48 or 49 in the case of an individual who is in the process of being cleared by DISCO) shall be placed in the "Name of Employee" block of the form. The individual's new name shall be set out in the "Remarks" block of the form. If the contractor has elected, under paragraph 26k(1)(b), to have Letters of Consent sent to a facility other than the one at which the individual is employed, the name and address of that facility shall be identified in the "Job Title" block.

- (4) Report of termination of employment (paragraphs 6a(4) and 6b(2)). Indicate "Termination (date)" in the "Remarks" block of the form.

- (5) Downgrading of a TOP SECRET clearance (see paragraph 30a. In the "Remarks" block indicate "Downgrade without prejudice to (SECRET or CONFIDENTIAL)."

- (6) Reinstatement of a previously downgraded TOP SECRET clearance (see paragraph 30b). In the "Remarks" block indicate "Reinstatement of previously downgraded TOP SECRET clearance due to a current requirement for access at such level."

c. It should be noted that where a contractor in a multiple facility organization elects, pursuant to paragraph 26k(1)(b), to have all Letters of Consent issued to the home office facility, the DLA Form 562-R will be utilized in the situations which call for the use of the form. In these cases, the name and

DoD 5220.22-M

address of the facility at which the individual is employed will be placed in the "Name and Address of Employer" block of the DLA Form 562-R. In addition, the name and

address of the facility to which Letters of Consent are mailed shall be placed in the "Job Title" block of the DLA Form 562-R (see paragraph 26k-(3)).

PERSONNEL SECURITY CLEARANCE CHANGE NOTIFICATION				FORM APPROVED BUDGET BUREAU NO. 199-R013	
1. TYPE OF ACTION <input type="checkbox"/> A. MULTIPLE FACILITY TRANSFER <input type="checkbox"/> B. REEMPLOYMENT <input type="checkbox"/> C. CHANGE OF NAME <input type="checkbox"/> D. TERMINATION					
2. TERMINATION STATUS (Complete if Item 1.d. is "X'd") <input type="checkbox"/> ACTIVE CLEARANCE <input type="checkbox"/> PENDING CLEARANCE AND <input type="checkbox"/> DD FORM 48 SUBMITTED <input type="checkbox"/> DD FORM 48-3 SUBMITTED					
3. NAME AND ADDRESS OF EMPLOYER			4. NAME OF EMPLOYEE (Last, First, Middle Name)		
			5. ANY OTHER NAME BY WHICH KNOWN (Alias, Maiden, or Former Legal Name; Designate which)		
6. DATE OF BIRTH		7. PLACE OF BIRTH		8. CITIZEN OF (Country)	
9. SOCIAL SECURITY NUMBER					
10. CURRENT LETTER OF CONSENT (Termination of Company Confidential should not be reported.)					
A. DEGREE OF CLEARANCE		B. DATE OF CLEARANCE		C. CLEARED BY	
11. IS EMPLOYEE CLEARED OR IN PROCESS FOR CLEARANCE IN CONNECTION WITH FACILITY SECURITY CLEARANCE (See Paragraph 22, ISM)? <input type="checkbox"/> YES <input type="checkbox"/> NO IF YES, ENTER JOB TITLE IN ITEM 12 AND SUBMIT THIS FORM TO COGNIZANT SECURITY OFFICE RATHER THAN DISCO.					
12. JOB TITLE (Complete this item only if Item 11 is answered YES)					
13. REMARKS (State appropriate information; i.e., Name and Address of Facility to which transferred; or "Termination," or New Name of Employee - Last Name, First Name, Middle Name; or Re-employment (include dates of termination and reemployment).)					
14. I certify that the entries made above are true, complete and correct to the best of my knowledge and belief. _____ SIGNATURE OF SECURITY SUPERVISOR DATE				FOR DISCO USE ONLY	
				_____ REINSTATED	
				_____ MULTI-FACILITY TRFD	
				_____ NO RECORD DISCO	
RETURN TO: _____					

R. Request for Administrative Termination of Personnel Security Clearance (DLA Form 683)

This form is used by contractors to request administrative termination of personnel security clearances that are no longer required. Government granted clearances and

contractor granted clearances can be administratively terminated for employees who no longer have or require access and will not require access in the foreseeable future. In the case of Government granted clearances the completed form is processed to DISCO, or, in the case of OODEPs, to the cognizant security office.

REQUEST FOR ADMINISTRATIVE TERMINATION OF PERSONNEL SECURITY CLEARANCE			
1. NAME, ADDRESS AND FEDERAL SUPPLY CODE OF EMPLOYER			
2. NAME OF EMPLOYEE (Last, First, Middle, Name) AND SSAN		3. ANY OTHER NAME BY WHICH KNOWN (Alias, Maiden or Former Legal Name; Designate which)	
4. DATE OF BIRTH	5. PLACE OF BIRTH	6. CITIZEN OF (Country)	
7. CURRENT PERSONNEL SECURITY CLEARANCE (Check and complete either A. or B., as appropriate)			
<input type="checkbox"/> A. GOVERNMENT GRANTED LETTER OF CONSENT:			
LEVEL OF CLEARANCE		DATE OF CLEARANCE	
Cleared by			
IS EMPLOYEE CLEARED (or in process for clearance) IN CONNECTION WITH FACILITY SECURITY CLEARANCE (See Paragraph 22, Industrial Security Manual)? <input type="checkbox"/> YES <input type="checkbox"/> NO IF YES, ENTER JOB TITLE AND SUBMIT THIS FORM TO COGNIZANT SECURITY OFFICE RATHER THAN DISCO. JOB TITLE:			
<input type="checkbox"/> B. CONTRACTOR GRANTED CONFIDENTIAL CLEARANCE ON: DATE			
8. I certify that the above named employee does not require access to classified information in connection with his (her) employment. Moreover, there will be no requirement for the employee to have access to classified information in the foreseeable future. Accordingly, it is recommended that the personnel security clearance be administratively terminated since there is no current or foreseeable future procurement requirement for the clearance. It is understood this recommendation is solely of an administrative nature and does not reflect adversely on the employee in any manner whatsoever. I certify that the entries made above are true, complete, and correct to the best of my knowledge and belief.			
A. SIGNATURE OF SECURITY SUPERVISOR		B. DATE	FOR DISCO USE ONLY
9. I certify that I do not currently have classified information in my possession or custody. My employer has advised me there will be no requirement for me to have access to classified information in the foreseeable future. Therefore I hereby acknowledge my employer's recommendation to administratively terminate the personnel security clearance which has been granted me. I understand that this termination is purely administrative in nature, it does not reflect adversely upon me in any manner whatsoever and further, that my employer may request a new personnel security clearance should the need arise in the future for me to have access to classified information.			
A. SIGNATURE OF WITNESS	B. DATE	C. SIGNATURE OF EMPLOYEE	D. DATE
RETURN TO: (NAME AND ADDRESS OF SUBMITTING FACILITY)			

**S. Envelope, Preaddressed to DISCO
(DLA Form 703)**

This form is an envelope used for submitting DD Form 48, DD Form 49, and DD Form 48-3 to DISCO. It enables a clearance applicant to put the form containing privileged information into the envelope and seal it.

address the envelope to his cognizant security office.

**T. Envelope, Not Preaddressed (DLA
Form 704)**

This form is an envelope used for submitting DD Form 48, DD Form 49, and DD Form 48-3 to the cognizant security office in OODEP cases. The contractor is required to

**U. Worksheet for the Preparation of Personnel Security Questionnaires, DD
Forms 48 or 49 (DLA Form 707)**

This worksheet is used by the employee in preparing a draft of the entries that will be inserted in Part I of the DD Form 48 or DD Form 49. This form cannot be offered to or required to be completed by an individual until he is employed by a contractor in a position requiring access to classified information and placed on the payroll.

WORKSHEET FOR PREPARATION OF PERSONNEL SECURITY QUESTIONNAIRE, DD FORMS 48 or 49				DATE																									
PART I	1. LAST NAME - FIRST NAME - MIDDLE NAME			2. SEX																									
	3. ALIAS(ES) AND ALL FORMER NAME(S)			4. SOCIAL SECURITY NUMBER																									
	5. MONTH, DAY, YEAR OF BIRTH	6. PLACE OF BIRTH		7. SERVICE NUMBER																									
<p>INSTRUCTIONS TO EMPLOYEE: This is a worksheet to assist in preparation of the final Personnel Security Questionnaire. The final version of the Personnel Security Questionnaire contains entries for additional information which you must complete in private. Part II of this worksheet need not be completed by your employer. It will be completed by your employer on the final version. After you complete this worksheet, give it to your employer so that it can be used as a guide for completion of the final version.</p> <p>TYPE OR PRINT ALL ANSWERS. If more space is required, attach additional sheets, identifying by corresponding block number. FORM WILL NOT BE ACCEPTED UNLESS COMPLETELY AND PROPERLY EXECUTED. Questions which do not apply shall be marked "None."</p>																													
<table border="1"> <thead> <tr> <th>8. RELATIVES</th> <th>DATE AND PLACE OF BIRTH</th> <th>PRESENT ADDRESS</th> <th>CITIZENSHIP</th> </tr> </thead> <tbody> <tr> <td>a. FATHER</td> <td></td> <td></td> <td></td> </tr> <tr> <td>b. MOTHER (Full Maiden Name)</td> <td></td> <td></td> <td></td> </tr> <tr> <td>c. SPOUSE (Full Maiden Name)</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>					8. RELATIVES	DATE AND PLACE OF BIRTH	PRESENT ADDRESS	CITIZENSHIP	a. FATHER				b. MOTHER (Full Maiden Name)				c. SPOUSE (Full Maiden Name)												
8. RELATIVES	DATE AND PLACE OF BIRTH	PRESENT ADDRESS	CITIZENSHIP																										
a. FATHER																													
b. MOTHER (Full Maiden Name)																													
c. SPOUSE (Full Maiden Name)																													
<p>9. RESIDENCES (List all from 18th birthday or during past 15 years, whichever is shorter. If under 18, list present and most recent addresses.)</p> <table border="1"> <thead> <tr> <th>a. FROM</th> <th>b. TO</th> <th>c. NUMBER AND STREET</th> <th>d. CITY</th> <th>e. STATE</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>					a. FROM	b. TO	c. NUMBER AND STREET	d. CITY	e. STATE																				
a. FROM	b. TO	c. NUMBER AND STREET	d. CITY	e. STATE																									
<p>10. EMPLOYMENT (List all from 18th birthday or during past 15 years, whichever is shorter. If under 18, list present and most recent employment)</p> <table border="1"> <thead> <tr> <th>a. FROM</th> <th>b. TO</th> <th>c. EMPLOYER</th> <th>d. PLACE</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>					a. FROM	b. TO	c. EMPLOYER	d. PLACE																					
a. FROM	b. TO	c. EMPLOYER	d. PLACE																										
<p>11. LAST CIVILIAN SCHOOL</p> <table border="1"> <thead> <tr> <th>a. FROM</th> <th>b. TO</th> <th>c. NAME</th> <th>d. PLACE</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>					a. FROM	b. TO	c. NAME	d. PLACE																					
a. FROM	b. TO	c. NAME	d. PLACE																										
<p align="center">PART II (TO BE COMPLETED BY EMPLOYER)</p> <table border="1"> <tr> <td colspan="2"> <p>TO:</p> <p>Defense Industrial Security Clearance Office Defense Supply Agency Box 2499 Columbus, Ohio 43216</p> </td> <td colspan="3"> <p>NAME AND ADDRESS OF EMPLOYER (If a subsidiary, include name of parent company)</p> </td> </tr> <tr> <td colspan="3"> <p>JOB TITLE AND DESCRIPTION OF EMPLOYEE'S DUTIES WHICH REQUIRE ACCESS TO CLASSIFIED INFORMATION</p> </td> <td colspan="2"> <p>CONTRACT NUMBER, WHEN APPLICABLE</p> </td> </tr> <tr> <td colspan="3"> <p>CLEARANCE REQUESTED IS: <input type="checkbox"/> INTERIM <input type="checkbox"/> UNDER PAR. 26f, ISM</p> </td> <td colspan="2"> <p>SECURITY CLASSIFICATION OF MATERIALS OR INFORMATION EMPLOYEE WILL HAVE ACCESS TO</p> </td> </tr> <tr> <td colspan="5"> <p>IF SUBJECT IS AN IMMIGRANT ALIEN, HAS HE PRESENTED ALIEN REGISTRATION RECEIPT CARD (Form I-151)?</p> <p><input type="checkbox"/> YES <input type="checkbox"/> NO</p> </td> </tr> <tr> <td colspan="3"> <p>I CERTIFY THAT THE ENTRIES MADE BY ME ABOVE ARE TRUE, COMPLETE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF AND ARE MADE IN GOOD FAITH.</p> </td> <td colspan="2"> <p>SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE</p> </td> </tr> </table>					<p>TO:</p> <p>Defense Industrial Security Clearance Office Defense Supply Agency Box 2499 Columbus, Ohio 43216</p>		<p>NAME AND ADDRESS OF EMPLOYER (If a subsidiary, include name of parent company)</p>			<p>JOB TITLE AND DESCRIPTION OF EMPLOYEE'S DUTIES WHICH REQUIRE ACCESS TO CLASSIFIED INFORMATION</p>			<p>CONTRACT NUMBER, WHEN APPLICABLE</p>		<p>CLEARANCE REQUESTED IS: <input type="checkbox"/> INTERIM <input type="checkbox"/> UNDER PAR. 26f, ISM</p>			<p>SECURITY CLASSIFICATION OF MATERIALS OR INFORMATION EMPLOYEE WILL HAVE ACCESS TO</p>		<p>IF SUBJECT IS AN IMMIGRANT ALIEN, HAS HE PRESENTED ALIEN REGISTRATION RECEIPT CARD (Form I-151)?</p> <p><input type="checkbox"/> YES <input type="checkbox"/> NO</p>					<p>I CERTIFY THAT THE ENTRIES MADE BY ME ABOVE ARE TRUE, COMPLETE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF AND ARE MADE IN GOOD FAITH.</p>			<p>SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE</p>	
<p>TO:</p> <p>Defense Industrial Security Clearance Office Defense Supply Agency Box 2499 Columbus, Ohio 43216</p>		<p>NAME AND ADDRESS OF EMPLOYER (If a subsidiary, include name of parent company)</p>																											
<p>JOB TITLE AND DESCRIPTION OF EMPLOYEE'S DUTIES WHICH REQUIRE ACCESS TO CLASSIFIED INFORMATION</p>			<p>CONTRACT NUMBER, WHEN APPLICABLE</p>																										
<p>CLEARANCE REQUESTED IS: <input type="checkbox"/> INTERIM <input type="checkbox"/> UNDER PAR. 26f, ISM</p>			<p>SECURITY CLASSIFICATION OF MATERIALS OR INFORMATION EMPLOYEE WILL HAVE ACCESS TO</p>																										
<p>IF SUBJECT IS AN IMMIGRANT ALIEN, HAS HE PRESENTED ALIEN REGISTRATION RECEIPT CARD (Form I-151)?</p> <p><input type="checkbox"/> YES <input type="checkbox"/> NO</p>																													
<p>I CERTIFY THAT THE ENTRIES MADE BY ME ABOVE ARE TRUE, COMPLETE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF AND ARE MADE IN GOOD FAITH.</p>			<p>SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE</p>																										

PART I (Continued)					
12. EDUCATION (Account for all civilian and military academies)					
YEARS (Month if known)		NAME AND LOCATION OF SCHOOL	GRADUATE		DEGREE
FROM	TO		YES	NO	
13. CITIZENSHIP					
ARE YOU A CITIZEN OF THE UNITED STATES? <input type="checkbox"/> YES <input type="checkbox"/> NO (If answer is "YES", complete Item a and b or c, if appropriate. If answer is "NO", complete Item d.)					
a. I AM A CITIZEN OF THE UNITED STATES BY REASON OF: <input type="checkbox"/> BY BIRTH IN THE UNITED STATES <input type="checkbox"/> BY NATURALIZED CITIZENSHIP * <input type="checkbox"/> BY BIRTH IN A FOREIGN COUNTRY OF UNITED STATES PARENTS <input type="checkbox"/> BY DERIVATIVE CITIZENSHIP *					
* If checked complete either "Citizenship by Naturalization" or "Citizenship by Derivation" Section below.					
b. CITIZENSHIP BY NATURALIZATION *					
WHERE NATURALIZED (City, County, State)				DATE NATURALIZED	
COURT				CERTIFICATE NUMBER	
c. CITIZENSHIP BY DERIVATION *					
PARENT'S NAME				PARENT'S CERTIFICATE NUMBER	
d. IMMIGRANT ALIENS ONLY COMPLETE THIS ITEM. U.S. CITIZENS SEE ITEM 13a.					
(1) ALIEN REGISTRATION NO.		(2) CITIZEN OF WHAT COUNTRY		(3) DATE AND PLACE OF LAST ENTRY INTO U.S.	
(4) DATE PETITION OF NATURALIZATION FILED		(5) DATE AND COURT OF ISSUANCE		(6) NUMBER	
(7) DO YOU INTEND TO BECOME A UNITED STATES CITIZEN?					
<input type="checkbox"/> YES <input type="checkbox"/> NO					
14. ORGANIZATIONAL MEMBERSHIP					
LIST ALL ORGANIZATIONS EXCEPT LABOR UNIONS AND EXCEPT ORGANIZATIONS REFERRED TO IN ITEM 27 BELOW IN WHICH YOU HOLD OR HAVE HELD MEMBERSHIP, IF NONE, SO STATE.					
NAME AND ADDRESS		TYPE	OFFICE HELD	FROM (Date)	TO (Date)
15. MILITARY SERVICE					
a. COUNTRY	BRANCH OF SERVICE		SERVICE NUMBER	FROM (Date)	TO (Date)
b. ARE YOU A MEMBER OF A RESERVE COMPONENT? <input type="checkbox"/> YES <input type="checkbox"/> NO (If answer is "YES", furnish service, component and current status under Item 21, "Remarks".)					
c. LOCAL DRAFT BOARD (United States) AND ADDRESS				d. SELECTIVE SERVICE NO.	e. CLASSIFICATION
16. PREVIOUS CLEARANCE					
a. HAVE YOU EVER BEEN PREVIOUSLY GRANTED A SECURITY CLEARANCE? (If answer is "YES", indicate level of clearance, when granted, by whom and where employed at that time under Item 21, "Remarks".) <input type="checkbox"/> YES <input type="checkbox"/> NO					
b. HAVE YOU EVER TERMINATED EMPLOYMENT WHILE A REQUEST OR APPLICATION FOR A SECURITY CLEARANCE WAS PENDING? (If answer is "YES", furnish name and address of employer under "Remarks". If termination resulted from a reduction in force, so indicate and furnish details under "Remarks". If you since have been granted a clearance by the Government, indicate under Item 21, "Remarks" the date, level of clearance and where employed.) <input type="checkbox"/> YES <input type="checkbox"/> NO					

17. OTHER RELATIVES				
a. LIST CHILDREN, BROTHERS, SISTERS (16 years and older) AND FORMER SPOUSE(S).				
RELATION	NAME IN FULL	ADDRESS (Enter "deceased" if no longer living)	PLACE AND DATE OF BIRTH	PRESENT CITIZENSHIP
b. LIST OTHER LIVING RELATIVES AND RELATIVES OF SPOUSE WHO ARE NOT UNITED STATES CITIZENS.				
18. FOREIGN COUNTRIES VISITED OR RESIDED IN				
CITY AND COUNTRY	DATE LEFT U.S.	DATE RETURNED U.S.	PURPOSE AND TYPE OF VISA	
19. LIST EACH FOREIGN GOVERNMENT, FIRM, CORPORATION OR PERSON FOR WHOM YOU ACT OR HAVE ACTED AS A REPRESENTATIVE, OFFICIAL OR EMPLOYEE IN THE PAST 5 YEARS. LIST ALL COMMUNIST GOVERNMENTS, FIRMS OR CORPORATIONS FOR WHOM YOU HAVE EVER ACTED IN SUCH CAPACITY. ATTACH A STATEMENT, AS REQUIRED BY PARAGRAPH 20k, ISM, FULLY DESCRIBING EACH AFFILIATION. (If none, so indicate.)				
20. REFERENCES (Give five personal references, stating business address of all references, if known. Do not include relatives, former employers, or persons living outside the United States.)				
NAME	YEARS KNOWN	STREET AND NUMBER	CITY	STATE
21. REMARKS (If additional space is needed, continue on plain paper.)				
<p>FURTHER INSTRUCTIONS: DO NOT COMPLETE PARTS III OR IV AT THIS TIME. Return this partially completed form to your employer who will review it to assure all entries are complete and the form is properly filled in. After return, proceed with completion of Parts III and IV.</p>				

DSA FORM 707
JAN 68

V. Facility Clearance Register (DD Form 1541) and Registration for Scientific and Technical Information Services (DD Form 1540)

The purpose of the DD Form 1541 is to provide for uniform certification of a facility's security clearance and safeguarding ability to the DDC, Cameron Station, Alexandria, Virginia, 22314, and to provide notice to DDC of changes affecting an existing certification.

a. For initial certifications, Part I of the form is executed by the contractor in accordance with instructions appearing on the form. It is forwarded in duplicate to the DCASR exercising security cognizance of the facility. The DCASR shall complete Part II of the form, noting in the "Remarks" section any limitations on the facility's eligibility to re-

ceive and store classified material. The original form, when certified, shall be forwarded to the DDC. The copy is to be retained as a part of the official facility security clearance records maintained by the DCASR. Contractors shall submit the DD Form 1541 only when requesting approval of the first DD Form 1540. When certified, the DD Form 1541 remains in effect for all future registrations or until changes occur affecting the clearance or safeguarding ability of the certified facility.

b. A copy of DD Form 1540 is included for information purposes. It is used to become eligible for the services of DDC and must be submitted to that office. Additional copies may be obtained from the following: DDC, Cameron Station, Alexandria, Virginia 22314, ATTN: DDC-TSR-I.

DoD 5220.22-M

FACILITY CLEARANCE REGISTER		
INSTRUCTIONS		
FOR CONTRACTOR: <ol style="list-style-type: none"> 1. Complete Part I in duplicate (<i>three copies if you desire a file copy</i>). 2. Forward two copies to the Defense Contract Administration Services Region (<i>DCASR</i>) having security cognizance over your company. 3. Separate facility clearance registers are required for each location to which classified material will be sent. 	FOR COGNIZANT DCASR: <ol style="list-style-type: none"> 1. Complete Part II. 2. Forward one copy to DDC at the address given below. 3. If you have no record of facility clearance, return forms to contractor with appropriate explanation. 	
PART I		
1. NAME AND MAILING ADDRESS OF FACILITY (<i>Classified material will be forwarded to this address</i>)	2. STREET ADDRESS (<i>Actual location if different from Item 1</i>)	
3. TYPED NAME AND TITLE OF REQUESTER	4. SIGNATURE	5. DATE
PART II		
6. THE FACILITY LISTED IN PART I IS CLEARED TO RECEIVE AND STORE DEPARTMENT OF DEFENSE CLASSIFIED MATERIAL UP TO AND INCLUDING <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input type="checkbox"/> SECRET <input type="checkbox"/> CONFIDENTIAL </div> <p style="font-size: small; margin-top: 5px;">(<i>Any change affecting this facility clearance will be reported immediately to DDC.</i>)</p>		
7. NAME AND ADDRESS OF THE DCASR	8. TYPED NAME AND TITLE OF CERTIFYING OFFICIAL	
	9. SIGNATURE	10. DATE
11. MAIL TO: Defense Documentation Center Cameron Station Alexandria, Virginia 22314		
REMARKS		

DD FORM 1541
1 SEP 65

REPLACES DDC FORM 62 WHICH IS OBSOLETE EFFECTIVE 1 JAN 1966

REGISTRATION FOR SCIENTIFIC AND TECHNICAL INFORMATION SERVICES (No carbon paper is required in the completion of this form)			FOR DDC CENTRAL FILE USE		APPROVING OFFICIAL FORWARD COMPLETED FORM TO: DEFENSE DOCUMENTATION CENTER ATTN: DDC-TSR-1 CAMERON STATION, BLDG. 5 ALEXANDRIA, VIRGINIA 22314
PART I - REQUESTER APPLICATION			DOD USER CODE		
1. ORGANIZATION NAME			CONTRACT TYPE		
2. MAILING ADDRESS (Street, City, State, ZIP Code)			USER TYPE		
3. ATTENTION LINE (Name and Organizational Title of Requesting Official)			FACILITY CLEARANCE		
5. SIGNATURE			CONTRACT CLEARANCE		
7. PRIME CONTRACT/GRANT OR PROGRAM NO. (Enter one only)			4. TELEPHONE NUMBER (Include Area Code)		
8. EXPIRATION DATE OF ITEM 7			5. DATE		
9. CLASSIFICATION REQUIRED			PART IV - SUBJECT FIELDS OF INTEREST		
<input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> NATO CLASSIFIED <input type="checkbox"/> CONFIDENTIAL <input type="checkbox"/> RESTRICTED DATA <input type="checkbox"/> SECRET <input type="checkbox"/> CNWDI			Circle required codes below. Mandatory only for Classified Services. First Number is the Subject Field; the second is the more specific group. See Subject Fields on Reverse.		
PART II - PRIME CONTRACTOR APPROVAL (If Part I is a Subcontractor)			01-01 06-12 11-01 15-05 19-04 01-02 06-13 11-02 15-06 19-05 01-03 06-14 11-03 15-07 19-06 01-04 06-15 11-04 16-01 19-07 01-05 06-16 11-05 16-02 19-08 02-01 06-17 11-06 16-03 20-01 02-02 06-18 11-07 16-04 20-02 02-03 06-19 11-08 16-04.1 20-03 02-04 06-20 11-09 16-04.2 20-04 02-05 06-21 11-10 16-04.3 20-05 02-06 07-01 11-11 17-01 20-06 03-01 07-02 11-12 17-02 20-07 03-02 07-03 12-01 17-02.1 20-08 03-03 07-04 12-02 17-03 20-09 04-01 07-05 13-01 17-04 20-10 04-02 08-01 13-02 17-05 20-11 05-01 08-02 13-03 17-06 20-12 05-02 08-03 13-04 17-07 20-13 05-03 08-04 13-05 17-08 20-14 05-04 08-05 13-06 17-09 21-01 05-05 08-06 13-07 17-10 21-02 05-06 08-07 13-08 18-01 21-03 05-07 08-08 13-09 18-02 21-04 05-08 08-09 13-10 18-03 21-05 05-09 08-10 13-10.1 18-04 21-06 05-10 08-11 13-11 18-05 21-07 05-11 08-12 13-12 18-06 21-08 06-01 08-13 13-13 18-07 21-08.1 06-02 08-14 14-01 18-08 21-08.2 06-03 09-01 14-02 18-09 21-09 06-04 09-02 14-03 18-10 21-09.1 06-05 09-03 14-04 18-11 21-09.2 06-06 09-04 14-05 18-12 22-01 06-07 09-05 15-01 18-13 22-02 06-08 09-06 15-02 18-14 22-03 06-09 10-01 15-03 19-01 22-04 06-10 10-02 15-03.1 19-02 06-11 10-03 15-04 19-03		
10. ORGANIZATION NAME AND ADDRESS			11. SUB-CONTRACT NUMBER		
13. TYPED NAME AND SIGNATURE			12. EXPIRATION DATE OF ITEM 11		
14. DATE			16. TELEPHONE NUMBER (Include Area Code)		
PART III - CERTIFICATION AND APPROVAL			17. DATE		
15. ORGANIZATION NAME AND ADDRESS			18. TYPED NAME AND TITLE OF APPROVING OFFICIAL		
19. SIGNATURE			19. SIGNATURE		
THE DDC CENTRAL FILES MUST BE NOTIFIED IMMEDIATELY OF ANY CHANGES TO INFORMATION PROVIDED ON THIS FORM					
(FOR DDC USE ONLY)					

SUBJECT FIELD AND GROUP STRUCTURE

- 01 Aeronautics**
 01 Aerodynamics
 02 Aeronautics
 03 Aircraft
 04 Aircraft flight instrumentation
 05 Air facilities
- 02 Agriculture**
 01 Agricultural chemistry
 02 Agricultural economics
 03 Agricultural engineering
 04 Agronomy and horticulture
 05 Animal husbandry
 06 Forestry
- 03 Astronomy and Astrophysics**
 01 Astronomy
 02 Astrophysics
 03 Celestial mechanics
- 04 Atmospheric Sciences**
 01 Atmospheric physics
 02 Meteorology
- 05 Behavioral and Social Sciences**
 01 Administration and management
 02 Documentation and information technology
 03 Economics
 04 History, law and political science
 05 Human factors engineering
 06 Humanities
 07 Linguistics
 08 Man-machine relations
 09 Personnel selection, training and evaluation
 10 Psychology (Individual and group behavior)
 11 Sociology
- 06 Biological and Medical Sciences**
 01 Biochemistry
 02 Bioengineering
 03 Biology
 04 Bionics
 05 Clinical medicine
 06 Environmental biology
 07 Escape, rescue and survival
 08 Food
 09 Hygiene and sanitation
 10 Industrial (Occupational) medicine
 11 Life support
 12 Medical and hospital equipment and supplies
 13 Microbiology
 14 Personnel selection and maintenance (Medical)
 15 Pharmacology
 16 Physiology
 17 Protective equipment
 18 Radiobiology
 19 Stress physiology
 20 Toxicology
 21 Weapon effects
- 07 Chemistry**
 01 Chemical engineering
 02 Inorganic chemistry
 03 Organic chemistry
 04 Physical chemistry
 05 Radio and radiation chemistry
- 08 Earth Sciences and Oceanography**
 01 Biological oceanography
 02 Cartography
 03 Dynamic oceanography
 04 Geochemistry
 05 Geodesy
 06 Geography
 07 Geology and mineralogy
 08 Hydrology and limnology
 09 Mining engineering
 10 Physical oceanography
 11 Seismology
 12 Snow, ice and permafrost
 13 Soil mechanics
 14 Terrestrial magnetism
- 09 Electronics and Electrical Engineering**
 01 Components
 02 Computers
 03 Electronic and electrical engineering
 04 Information theory
 05 Subsystems
 06 Telemetry
- 10 Energy Conversion (Non-propulsive)**
 01 Conversion techniques
 02 Power sources
 03 Energy storage
- 11 Materials**
 01 Adhesives and seals
 02 Ceramics, refractories and glasses
 03 Coatings, colorants and finishes
 04 Composite materials
 05 Fibers and textiles
 06 Metallurgy and metallography
 07 Miscellaneous materials
 08 Oils, lubricants, and hydraulic fluids
 09 Plastics
 10 Rubbers
 11 Solvents, cleaners and abrasives
 12 Wood and paper products
- 12 Mathematical Sciences**
 01 Mathematics and statistics
 02 Operations research
- 13 Mechanical, Industrial, Civil and Marine Engineering**
 01 Air conditioning, heating, lighting and ventilating
 02 Civil engineering
 03 Construction equipment, materials and supplies
 04 Containers and packaging
 05 Couplings, fasteners and joints
 06 Ground transportation equipment
 07 Hydraulic and pneumatic equipment
 08 Industrial processes
 09 Machinery and tools
 10 Marine engineering
 10.1 Submarine engineering
 11 Pumps, filters, pipes, tubing and valves
 12 Safety engineering
 13 Structural engineering
- 14 Methods and Equipment**
 01 Cost effectiveness
 02 Laboratories, test facilities, and test equipment
 03 Recording devices
 04 Reliability
 05 Reprography
- 15 Military Sciences**
 01 Antisubmarine warfare
 02 Chemical, biological, and radiological warfare
 03 Defense
 03.1 Antimissile defense
 04 Intelligence
 05 Logistics
 06 Nuclear warfare
 07 Operations, strategy, and tactics
- 16 Missile Technology**
 01 Missile launching and ground support
 02 Missile trajectories
 03 Missile warheads and fuzes
 04 Missiles
 04.1 Air and space launched missiles
 04.2 Surface launched missiles
 04.3 Underwater launched missiles
- 17 Navigation, Communications, Detection and Countermeasures**
 01 Acoustic detection
 02 Communications
 02.1 Radio communications
 03 Direction finding
 04 Electromagnetic and acoustic countermeasures
 05 Infrared and ultraviolet detection
 06 Magnetic detection
 07 Navigation and guidance
 08 Optical detection
 09 Radar detection
 10 Seismic detection
- 18 Nuclear Science and Technology**
 01 Fusion devices (Thermonuclear)
 02 Isotopes
 03 Nuclear explosions
 04 Nuclear instrumentation
 05 Nuclear power plants
 06 Radiation shielding and protection
 07 Radioactive wastes and fission products
 08 Radioactivity
 09 Reactor engineering and operation
 10 Reactor materials
 11 Reactor physics
 12 Reactors (Power)
 13 Reactors (Non-power)
 14 SNAP technology
- 19 Ordnance**
 01 Ammunition, explosives and pyrotechnics
 02 Bombs
 03 Combat vehicles
 04 Explosions, ballistics and armor
 05 Fire control and bombing systems
 06 Guns
 07 Rockets
 08 Underwater ordnance
- 20 Physics**
 01 Acoustics
 02 Crystallography
 03 Electricity and magnetism
 04 Fluid mechanics
 05 Masers and lasers
 06 Optics
 07 Particle accelerators
 08 Particle physics
 09 Plasma physics
 10 Quantum theory
 11 Solid mechanics
 12 Solid state physics
 13 Thermodynamics
 14 Wave propagation
- 21 Propulsion and Fuels**
 01 Air breathing engines
 02 Combustion and ignition
 03 Electric propulsion
 04 Fuels
 05 Jet and gas turbine engines
 06 Nuclear propulsion
 07 Reciprocating engines
 08 Rocket motors and engines
 08.1 Liquid rocket motors
 08.2 Solid rocket motors
 09 Rocket propellants
 09.1 Liquid rocket propellants
 09.2 Solid rocket propellants
- 22 Space Technology**
 01 Astronautics
 02 Spacecraft
 03 Spacecraft trajectories and reentry
 04 Spacecraft launch vehicles and ground support

**W. Letter Agreement to Safeguard
Classified Information for an Employee
Performing Consultant Services**

This agreement shall be prepared and executed by a contractor if he agrees to accept responsibility for safeguarding classified in-

formation released to his employee furnishing consultant services.

The contractor shall send the original to his cognizant security office and effect such other distribution as indicated on the agreement. In case of failure to execute this agreement, the consultant shall be cleared as a facility.

(Company Letterhead)

To: (Date)
(Cognizant Security Office)

Gentlemen:

In accordance with paragraph 70 of the Industrial Security Manual for Safeguarding Classified Information (ISM), the cleared to the level of and
(name of cleared facility) (level of facility clearance) (name of employee)
an employee cleared for access to classified information, by on
(level) (activity granting clearance) (date)
who is serving as a consultant to hereby jointly agree:
(name of using facility or User Agency activity)

- (i) To place classified material received and/or produced by said employee in his capacity as a consultant into the facility's classified material control system.
- (ii) To provide the employee with an approved container in which to store classified material relating to his consulting activity.
- (iii) To incorporate procedures in the facility's Standard Practice Procedure implementing the access limitation requirements of paragraphs 70a(2) and (8), ISM.
- (iv) To abide by the procedures of the facility's Standard Practice Procedure in handling classified material relating to the employee's consulting activity.
- (v) To advise the cognizant security office and the contractor or User Agency activity to which the employee is a consultant of any change in the consultant's status as an employee of the facility.

.....
(Employee-Consultant Signature) (Employing Contractor Signature)
.....
(Date) (Title)
.....
(Date) (Date)

Copy to:

Facility of Employee Consultant
Contractor or User Agency to which Employee is Consultant
Employee Consultant

Appendix I

APPENDIX II

DOWNGRADING AND DECLASSIFICATION

This Appendix prescribes a progressive system for the downgrading or declassification of classified information on a time-phased basis. This Appendix is not a guide for the assignment of a classification to information; it applies only to official information which has been assigned a security classification by competent authority.

A. Scope and Application

1. *General.* Executive Order 11652 prescribes that when classified information is determined, in the interest of national security, to require a different level of protection than that presently assigned, or no longer requires any such protection, it shall be regraded or declassified, in order to preserve the effectiveness and integrity of the classification system and to eliminate unnecessary classification.

2. *User Agency Information.* In compliance with their responsibilities under the above E.O., the Secretaries of Defense, Commerce, State, Treasury, Transportation, Interior, Agriculture, Labor, and Health, Education and Welfare; the Attorney General, Department of Justice; the Administrators, General Services Administration, Small Business Administration, National Aeronautics and Space Administration, Environmental Protection Agency, and Federal Energy Administration; and the Directors, National Science Foundation and U.S. Arms Control and Disarmament Agency (all hereinafter referred to as User Agencies) have prescribed that the provisions of this Appendix shall apply to all classified information (see paragraph 3g) originated in the User Agencies or by one of their components or contractors. This encompasses all classified information originated by the Office of the Secretary of Defense and DoD agencies; the present and former Joint Chiefs of Staff and

Joint Staff; the Department of Army and former War Department; the Department of Navy; the Department of Air Force and former Army Air Forces; the U.S. Coast Guard when acting as a part of Navy, Treasury or Transportation; in NASA and predecessor NASA agencies, including the National Advisory Committee for Aeronautics; in the FAA, prior and subsequent to its assignment to the Department of Transportation, predecessor FAA agencies, including the Civil Aeronautics Administration and the Airways Modernization Board, formerly of the Department of Commerce; joint committees or agencies comprised entirely of representatives from within the above-described agencies or their predecessor agencies; other Government agencies whose functions have officially transferred to any of the above agencies; and contractors in the performance of contracts awarded by or on behalf of the User Agencies, their components or their predecessors.

3. *Authority of Contractors.* The contractor shall apply and implement the provisions of this Appendix unless otherwise instructed by his contracting officer.¹ In those cases in which a contracting officer determines that the material has been improperly

¹ In those cases in which a contractor receives instructions which appear to be in conflict with the provisions of this Appendix, the contractor shall immediately notify the contracting officer of the conflicting instructions. Pending resolution of the problem, he shall comply with the most recent instructions received from the contracting officer.

designated, the contracting officer shall instruct the contractor to mark the material to reflect the correct designation.

4. *Responsibility of Contractors.* Each contractor who possesses classified material affected by this Appendix is responsible for initiating action to apply the appropriate notation and to change or cancel classifications as prescribed herein. If a contractor receives classified material other than RESTRICTED DATA or FORMERLY RESTRICTED DATA, which does not bear a downgrading and declassification marking he shall mark the material for the GDS (see paragraphs B2 and C2, below), and so notify the originator. Such actions are the responsibility of each holder of classified material; they constitute an implementation of a directed action rather than an exercise of the authority for deciding the change or cancellation of a classification.¹ Pending the remarking of classified material, as prescribed in this Appendix, the contractor shall safeguard the material in accordance with the classification marked on it.

5. *Requests for Advice.* When the contractor cannot determine exactly which provision of this Appendix applies to certain classified information or material, he shall request advice from the contracting officer concerned. If the contracting officer is unknown, or is known to have been abolished, such requests will be forwarded through User Agency contracting channels, as appropriate. If the channels are not known, the request will be sent directly to the appropriate office shown below. All such requests must include a complete description or identification of the classified information or document in question.

a. *OSD.* Deputy Assistant Secretary of Defense (Security Policy), ATTN: Director, Information Security Division, The Pentagon, Washington, D.C. 20301.

b. *Army.* The Adjutant General, ATTN: DAAG-AMR-S, Department of Army, Washington, D.C. 20315.

c. *Navy.* Chief of Naval Material, ATTN: NMAT 05, Washington, D.C. 20360.

d. *Air Force.* Headquarters, USAF, ATTN: AF/SPIB, Washington, D.C. 20314.

e. *NASA.* Headquarters, NASA, ATTN: Code ADA-42, Washington, D.C. 20546.

f. *Commerce.* Director of Investigations and Security, Department of Commerce, Washington, D.C. 20230.

g. *GSA.* Director, Security Division, Office of Investigations, General Services Administration, Washington, D.C. 20405.

h. *State.* Director of Security, Department of State, Washington, D.C. 20230.

i. *SBA.* Director, Office of Security and Investigations, Small Business Administration, Washington, D.C. 20416.

j. *NSF.* Security Officer, National Science Foundation, Washington, D.C. 20550.

k. *Treasury.* Departmental Physical Security Officer, Department of Treasury, Washington, D.C. 20220.

l. *Transportation.* Chief, Security Division, Department of Transportation, Washington, D.C. 20590.

m. *Interior.* Defense Coordinator, Department of The Interior, Washington, D.C. 20240.

n. *Agriculture.* Department Security Officer, Department of Agriculture, Washington, D.C. 20250.

o. *HEW.* Director of Security, Department of Health, Education and Welfare, Washington, D.C. 20201.

p. *Labor.* Chief, Physical Security Branch, Office of the Assistant Secretary for

Administration, Department of Labor, Washington, D.C. 20210.

q. *EPA*. Director, Security and Inspections Staff, Environmental Protection Agency, Washington, D.C. 20460.

r. *FEA*. Director, Office of Security, Inspections and Audits, Federal Energy Administration, Washington, D.C. 20416.

s. *Justice*. Director, Security and Administrative Programs Staff, Office of Management and Finance, Department of Justice, Washington, D.C. 20530.

t. *ACDA*. Security Officer, U.S. Arms Control and Disarmament Agency, Washington, D.C. 20451.

B. Automatic Downgrading and Declassification

All material classified on or after June 1, 1972, is subject to automatic downgrading and declassification except in those instances in which an exemption from the GDS is granted by a Government official designated to exercise TOP SECRET classification authority. Automatic downgrading and declassification shall conform to the following requirements.²

1. *Advanced Declassification Schedule*. Government officials exercising classification authority are required, concurrently with making classification determinations, to identify specific future dates or events for automatic downgrading and declassification in all cases where it is possible to do so. These dates or events shall be as early as the national security will permit. In the DoD, the GDS, as set forth in paragraph 2 below, shall

² The date of the initial specification, drawing, or blueprint from which hardware is manufactured may be used as the date from which to compute automatic downgrading or declassification of the information which may be disclosed by the hardware.

not be used unless an ADS for a date or event earlier than the GDS cannot be determined. The marking for an ADS is as follows:

SECRET on _____	(effective date)
CONFIDENTIAL on _____	(effective date)
DECLASSIFY on _____	(effective date)
CLASSIFIED BY _____	

2. *General Declassification Schedule*. When earlier dates or events for downgrading and declassification have not been determined, the following shall apply:

a. *TOP SECRET*. Information or material originally classified TOP SECRET shall be automatically downgraded to SECRET at the end of the second full calendar year following the year in which it was originated, and shall be downgraded to CONFIDENTIAL at the end of the fourth full calendar year following the year in which it was originated, and shall be declassified at the end of the tenth full calendar year following the year in which it was originated. For example, a document classified TOP SECRET on 1 June 1972 will automatically be downgraded to SECRET on 31 December 1974, downgraded to CONFIDENTIAL on 31 December 1976, and declassified on 31 December 1982.

b. *SECRET*. Information and material originally classified SECRET shall be automatically downgraded to CONFIDENTIAL at the end of the second full calendar year following the year in which it was originated, and shall be declassified at the end of the eighth full calendar year following the year in which it was originated.

c. *CONFIDENTIAL*. Information and material originally classified CONFIDENTIAL

TIAL shall be automatically declassified at the end of the sixth full calander year following the year in which it was originated.

d. *Marking.* The marking for the GDS is as follows:

<p>CLASSIFIED BY _____ SUBJECT TO GDS of E.O. 11652 AUTOMATICALLY DOWNGRADED AT TWO-YEAR INTERVALS DECLASSIFIED ON DECEMBER 31, _____ (year)</p>
--

3. *Method of Marking.* The ADS or GDS marking, as appropriate, shall be typed, stamped, printed, or otherwise clearly and conspicuously affixed at the bottom of the first or title page, or in a similarly prominent place immediately below or adjacent to and in conjunction with the classification marking.

C. Material Exempted From the GDS

A Government official who is authorized to exercise TOP SECRET classification authority may designate classified material or information at any level, originated by him or under his supervision, as exempt from the GDS. In each case, this official shall specify in writing on the material, or by other written direction issued in advance, the exemption category claimed (see paragraph 1, below). Unless it is impossible to do so, a date or event for automatic declassification of the material earlier than 30 years from the date of origin shall be specified concurrently with the determination to grant an exemption.

1. *Exempt Categories.*

a. *Category (1).* Classified information or material furnished by foreign organizations and held by the U.S. on the understanding that it be kept in confidence.

b. *Category (2).* Classified information or material specifically covered by statute or pertaining to cryptography, or disclosing intelligence sources or methods.

c. *Category (3).* Classified information or material disclosing a system, plan, installation, project, or a specific foreign relations matter, the continuing protection of which is essential to the national security.

d. *Category (4).* Classified information or material, the disclosure of which would place a person in immediate jeopardy.

2. *Method of Marking.* Material or information designated as being exempt (except material marked RESTRICTED DATA or FORMERLY RESTRICTED DATA) shall have typed, stamped, printed or otherwise clearly and conspicuously marked at the bottom of the first page or title page, or in a similarly prominent place immediately below or adjacent to and in conjunction with the classification marking, the following notation:

<p>CLASSIFIED BY _____ EXEMPT FROM GDS OF E.O. 11652 EXEMPTION CATEGORY _____ DECLASSIFIED ON _____ (effective date)</p>
--

RESTRICTED DATA or FORMERLY RESTRICTED DATA material will be marked in accordance with paragraph 11b(2) or 11b(3), and the CLASSIFIED BY line will be completed as indicated in paragraph D1 below.

D. Completion of CLASSIFIED BY, DECLASSIFY ON, and EXEMPTION CATEGORY Spaces

1. *Classified By.*

a. In completing the CLASSIFIED BY line, the contractor shall identify the applicable DD Form 254 (see paragraph *b*, below). In addition, if any single guidance source other than or in addition to the applicable DD Form 254 is followed, that source will also be shown in such a way that, standing alone, it will be sufficiently complete to identify it, including its date and the title and organization of the original classifier when known. If two or more guidance sources other than or in addition to the applicable DD Form 254 are followed, the identification of the DD Form 254 will be followed by the phrase "and other applicable guidance sources" (e.g., DD Form 254, 30 June 1972, RFQ #12345, and other applicable guidance sources). In each such case when the phrase, "and other applicable guidance sources," is used, the contractor will maintain adequate records to support the application of the classification marking, and will retain such records for the duration of the contract or program under which the document was created. The records could take the form of a bibliography identifying the applicable classification sources and be keyed to the text, or could be a notation on the contractor's record copy of the classified document to clearly identify the classification sources involved.

b. Identification of the applicable DD Form 254 in the CLASSIFIED BY line will always include at least the following:

(1) The date of the DD Form 254, and

(2) The specific designator (e.g., contract number) of the contract or other requirements document for which the DD Form 254 was issued.³

2. *Declassify On.* This space will be completed in accordance with the instructions

contained in the classification guidance source or sources identified in the CLASSIFIED BY line referred to in paragraph 1a, above.

3. *Exemption Category.* This space will be completed by entering the category; for example "(1)". The number designation of the exemption category will be obtained from the guidance source(s) identified in the CLASSIFIED BY line referred to in paragraph 1a, above.

E. Electrically Transmitted Messages

The provisions of this Appendix apply to all messages as well as to any other form of recorded information. It is not necessary that a classified message be marked with a CLASSIFIED BY line. However, the last line or paragraph of every classified message shall show either:

1. "ADS (insert date or event)" Advanced Declassification Schedule (see paragraph B1, above) for date or event earlier than the General Declassification Schedule;

2. "GDS (insert last two digits of declassification year)" for General Declassification Schedule (see paragraph B2, above) cases; or

3. "XGDS (insert exemption category number(s)) (Insert last two digits of declassification year if known for exemption cases (see paragraph C1, above).)" For example, a message containing intelligence sources or methods information which is scheduled for declassification 30 years from

³ For potential prime contractors responding to an IFB, RFQ, or RFP, when no contract designator is shown in item 3a of the DD Form 254, the designator shown in item 3c of the DD Form 254 shall be used. Prime contractors and subcontractors at all tiers shall use the designator set forth in item 3a of the DD Form 254. If future experience should show that the date of the DD Form 254 and the specific designator are not adequate for efficient administration, additional identification may later be required.

DoD 5220.22-M

the 1973 date of origin would show "XGDS(2)(03)."

4. "XCL (insert last two digits of downgrading year)" for a message containing information which is excluded from the GDS. NOTE: Such messages will not be automatically declassified (see paragraph F2, below). Upon receipt of notification of declassification, contractors need not remove the date time group from electrically transmitted messages or paraphrase such messages, notwithstanding the fact that such instructions may be noted therein.

F. Re-marking Pre-June 1, 1972 Material

1. If the pre-June 1, 1972 material was marked Group 1 or 2, or was not group marked at all, it will be re-marked as follows:

EXCLUDED FROM THE GDS

2. If the pre-June 1, 1972 material was marked Group 3, re-marking is not necessary. However, if the material has already been re-marked "Excluded From the GDS" as previously required, such marking need not be cancelled or obliterated. The Group 3 material shall continue to be downgraded at 12-year intervals from the date of origin until it reaches the classification level of CONFIDENTIAL. The Group 3 material will not be automatically declassified.

3. If the pre-June 1, 1972 material was marked Group 4, it will be re-marked for the GDS, except that it will be marked for exemption from the GDS if the material has been exempted and notice of the exemption has been received. The date of origin is the starting date for the GDS, until such time as notice of downgrading or declassification or other change of status is received.

G. Marking New Material Prepared on or After June 1, 1972, Based on Pre-June 1, 1972 Source Material, or a Pre-June 1, 1972 Classification Guide Which Has Not Been Revised to Reflect E.O. 11652

1. If the guidance source is pre-June 1, 1972 documents or material, all new material shall be marked as follows:

a. If the guidance source is marked Group 1 or 2, or not group marked at all (material which should be marked "Excluded From the GDS"), any new material the classification of which is based on such guidance source will be marked as follows:

CLASSIFIED BY:

EXCLUDED FROM THE GDS

b. If the guidance source is marked Group 3, the marking set forth in paragraph 2b, below, shall be placed on the new material. The new material shall be downgraded at 12-year intervals starting from the date of the source document or material.

c. If the guidance source is marked Group 4 (which should be re-marked for the GDS), the new material will be marked for the GDS. The date of origin of the pre-June 1, 1972 material is the starting date for the GDS.

2. If the guidance source is a pre-June 1, 1972 DD Form 254 or other classification guide, new material generated shall be marked as follows:

a. If the DD Form 254 or other classification guide designated the material for Group 1 or 2, or did not designate it for any group, the new material will be marked as follows:

CLASSIFIED BY:
EXCLUDED FROM THE GDS

b. If the DD Form 254 or other classification guide designated the material for Group 3, the new material shall have the ADS marking affixed and completed as follows:

SECRET on: (enter date 12 years from date of pre-June 1, 1972 source material or classification guidance.)

CONFIDENTIAL on: (enter date 12 years from date of origin as SECRET, or date of downgrading from TOP SECRET to SECRET.)

DECLASSIFY on: (enter the statement, "Not Automatically Declassified.")

CLASSIFIED by: (complete this entry in accordance with paragraph D1.)

c. If the DD Form 254 or other classification guide designated the material for Group 4, the new material will be marked for the GDS. The date of the classification guidance is the starting data for the GDS for such material.

H. Most Restrictive Marking Determination

When a document or material prepared subsequent to 1 June 1972 includes classified information, either newly developed or extracted from one or more sources, which is designated under more than one of the provisions of paragraph B or C above, the single downgrading and declassification marking assigned the document or material shall be the most restrictive of those which are applicable to the information contained there-

in. Most restrictive, in this instance, means that marking which protects the material in accordance with the longer appropriate time frame involved. For example, if one source document indicates downgrading shall be in accordance with the GDS, while another source document indicates the material is to be downgraded at an earlier date, the provisions of the GDS shall apply. When more than one category of exempt material is involved, the exemption notation shall identify all such categories.

I. Dates or Events Carried Forward

Downgrading or declassification dates or events required on markings as set forth in paragraph B1, B2, C2, or G2 of this Appendix shall be carried forward and applied whenever the classified information is incorporated in documents or other material originated at a later date.

J. Changing Classification Markings

At the time the material is actually downgraded or declassified, the action to change the classification markings shall be initiated and performed in accordance with the provisions of paragraph 11c. When classification markings are changed or cancelled, an entry, when appropriate, shall be made in the control station records prescribed in paragraph 12, to reflect such change or cancellation.

K. Re-Marking Pre-June 1, 1972 Material On Hand

Pre-June 1, 1972 material on hand shall be re-marked in accordance with the above guidelines when it is taken from file or storage for any use.

L. Release of Declassified Information

Declassification, either automatically or by individual review and determination, is not automatically an approval for public release. Accordingly, contractors shall request approval for public release of "declassified" information in accordance with the provisions of paragraph 50.

APPENDIX III

FOREIGN CLASSIFIED CONTRACTS

Table Outlining Responsibilities for Security Actions

Certain duties which this Manual assigns to the contracting officer or to the contracting User Agency are, with respect to foreign classified contracts, assigned to the EDIS, HQ DLA; the administrative contracting office; or to the cognizant security office.

Table I shows the assignment of these duties. Contractors will submit their requests for instructions or guidance as set forth below. Duties not specifically assigned herein are reserved to the foreign government agency or foreign contracting activity concerned. Requests for instructions in such cases shall be submitted through the EDIS, HQ DLA.

TABLE 1

Action	References	EDIS, HQ DLA	Administrative Contracting Officer	Cognizant Security Office
1. Approves retention of classified information by contractor or subcontractor.	Pars. 5l, 5m, and 64, ISM.		x	
2. Authorizes and provides instruction for transmission of classified information outside the facility.	Pars. 5 and 17, ISM.		x	x
3. Authorizes reproduction of classified information.	Par. 18, ISM		x	
4. Authorizes destruction of certain classified information.	Par. 19, ISM		x	
5. Approval of electrical alarm service	Pars. 35 and 36, ISM.		x ²	x
6. Approves controlled areas	Par. 34, ISM		x ²	x
7. Approves visits for Categories 2 and 3 visitors ..	Par. 41, ISM		x ¹	x
8. Authorizes disclosure of TS information to subcontractor.	Par. 59, ISM		x	
9. Receives notification of award of classified subcontract. ³	Par. 62, ISM	x	x	x
10.				
a. Approves Security Classification Guidance for subcontracts.	Par. 60, ISM		x	
b. Obtains Security Classification Guidance for subcontracts.		x		

¹ Some foreign contracts will be managed by foreign personnel directly from the country concerned, their Washington Embassy or other means with no U.S. contracting officer involved. U.S. User Agencies control Category 4 type visits as well as Category 3. Necessary coordination will be effected with the EDIS, HQ DLA, the cognizant security office and the contractor concerned.

² If costs are involved.

³ This notice shall be sent to the cognizant security office of the subcontractor.

APPENDIX IV

OUTLINE CONSTRUCTION SPECIFICATIONS FOR STORAGE VAULTS

A. Application

The following outline specifications are the criteria for the construction of vaults and strongrooms for use as storage facilities for classified material under the conditions stipulated in paragraph 14 of this Manual. Vaults ordered constructed after 1 July 1966 shall conform to these specifications. Vaults equipped with doors that do not meet Federal or interim Federal Specifications (GSA-FSS), Door, Vault, Security shall require the supplemental controls prescribed in paragraph 14a(3)(f).

B. Class A Vault

1. *Floor and Walls.* Eight-inch-thick reinforced concrete. Walls to extend to the underside of the roof slab above.

2. *Roof.* Monolithic reinforced-concrete slab of a thickness to be determined by structural requirements, but not less thick than the walls and floors.

3. *Ceiling.* Where the underside of the roof slab or roof construction exceeds 12 feet in height, or where the roof construction is not in accordance with paragraph 2 above, a normal reinforced-concrete slab will be placed over the vault area at a height not to exceed 9 feet.

4. *Vault Door and Frame Unit.* The vault door and frame unit shall be one originally procured from the FSS.¹

5. *Lock and Locking Parts.* The lock shall

¹ Vault door-in-frame units are listed in the FSS (FSC Group 71, Part XI). Copies of the schedule may be obtained from any regional office of the GSA.

conform to Underwriters' Standard No. 768 Group I-R. It shall be equipped with a "top-reading, spy-proof type dial." The UL label is considered adequate evidence of compliance with these requirements. Axial play on the level handle spindle shall not exceed 1/16". The locks, lock bolt, door bolt operating cam, and bolt operating linkage connected thereto shall be protected by a tempered steel alloy hardplate located in front of the parts to be protected. Such hardplate to be at least 1/4" in thickness and to be in the Rockwell hardness range of C-63 to C-65. The front plate, edge plates, back plates, and cap sheet shall be of manufacturer's standard construction. The cap sheet of the door will have an inspection plate of such size that its removal will permit examination and inspection of the combination lock and operating cam area without removal of entire back cap sheet of the door.

C. Class B Vault

1. *Floor.* Monolithic concrete construction of the thickness of adjacent concrete floor construction, but not less than four inches thick.

2. *Walls.* Not less than 8-inch-thick brick, concrete block, or other masonry units. Hollow masonry units shall be the vertical cell type (load bearing) filled with concrete and steel reinforcement bars. Monolithic steel-reinforced concrete walls at least four inches thick may also be used, and shall be used in seismic areas.

3. *Roof.* Monolithic reinforced-concrete slab of a thickness to be determined by structural requirements.

4. *Ceiling.* Where the underside of the room slab exceeds 12 feet in height or where roof construction is not in accordance with paragraph 3 above, a normal reinforced-concrete slab will be placed over the vault at a height not to exceed nine feet.

5. *Vault Door and Frame Unit.* See paragraph B4.

6. *Lock.* See paragraph B5.

D. Class C Vault

1. *Floor.* See paragraph C1.

2. *Walls.* Not less than 8-inch-thick hollow clay tile (vertical cell double shell) or concrete block (thick shell). Monolithic steel-reinforced-concrete walls at least four inches thick may also be used, and shall be used in seismic areas. Walls back of the exterior wall-faction of the building shall be concrete, solid masonry, or hollow masonry units filled with concrete and steel reinforcement bars.

3. *Roof.* See paragraph C3.

4. *Ceiling.* See paragraph C4.

5. *Vault Door and Frame Unit.* See paragraph B4.

6. *Lock.* See paragraph B5.

E. Structural Design

In addition to the requirements given above, the wall, floor, and roof construction shall be in accordance with nationally recognized standards of structural practice. For the vaults described above, the concrete shall be poured in place, and will have a minimum 28-day compressive strength of 2,500 psi.

F. Strongrooms

A strongroom, as referred to in paragraph 14a(3)(f), shall be considered to be an in-

terior space enclosed by, or separated from other similar spaces by, four walls, a ceiling and a floor, all of which are constructed of solid building materials. Under this criteria, rooms having false ceiling and walls constructed of fabrics, wire mesh or other similar material shall not qualify as a strong-room. Specific construction standards are as follows:

1. *Hardware.* Heavy-duty builder's hardware shall be used in construction, and all screws, nuts, bolts, hasps, clamps, bars, hinges, pins, etc., shall be securely fastened to preclude surreptitious entry and assure visual evidence of forced entry. Hardware accessible from outside the area shall be peened, brazed or spot welded to preclude removal.

2. *Walls and Ceilings.* Construction shall be of plaster, gypsum board, metal, hard-board, wood, plywood or other materials offering similar resistance to, or evidence of, unauthorized entry into the area. Insert type panels shall not be used.

3. *Floor.* Floors shall be of solid construction, utilizing materials such as concrete, ceramic tile, wood, etc.

4. *Windows.* Window openings less than 18 feet above the ground or less than 14 feet directly or diagonally opposite uncontrolled windows in other walls, fire escapes and roofs shall be fitted with $\frac{1}{2}$ " bars (separated by no more than 6"), plus cross bars to prevent spreading or wire mesh securely fastened on the inside. In addition to being kept closed at all times, the window shall be translucent or opaqued by any practical method, such as paint on both sides of the window, tempered masonite, sheet metal, cement-asbestos board, etc.

5. *Miscellaneous Openings.* Where ducts, registers, sewers and tunnels are of such size and shape as to permit unauthorized entry or visual access, they shall be equipped with man-safe barriers such as wire mesh (No. 9

gauge, 2 inch square mesh) or steel bars of at least $\frac{1}{2}$ " in diameter extending across their width with a maximum space of 6" between the bars. The steel bars shall be securely fastened at both ends to preclude removal, with cross bars to prevent spreading. Where wire mesh or steel bars are used, care shall be exercised to insure that classified material within the room cannot be removed with the aid of any type of instrument. Door traps shall be dead-bolted inside the room.

6. *Doors.* Doors shall be substantially constructed of wood or metal. When windows, panels or similar openings are used, they shall be secured with wire mesh securely

fastened on the inside. The windows shall be translucent or opaqued. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

7. *Door Louvers and Baffle Plates.* When used, they shall be reinforced with wire mesh (No. 9 gauge, 2 inch square mesh) fastened inside the room.

8. *Door Locking Devices.* Doors shall be secured by either a built-in, three-position, dial-type, changeable combination lock, or a three-position, dial-type, changeable combination padlock as specified in paragraph 14a (3) (d), which is secured to the door by a solid metal hasp.

APPENDIX V

GUIDELINES FOR THE PHYSICAL CONSTRUCTION OF CLOSED AREAS

A. Application

The following guidance is offered to contractors as a reasonable norm to evaluate the adequacy of existing structural safeguards for Closed Areas and to provide guidance for construction of new areas.

B. Guidance

1. *Hardware.* Heavy-duty builders' hardware should be used in construction, and all screws, nuts, bolts, hasps, clamps, bars, two-inch square mesh of No. 9 (Federal Specification RR-F-191d, June 17, 1965) wire, hinges, pins, etc., should be securely fastened to preclude surreptitious removal and assure visual evidence of tampering. Hardware accessible from outside the area should be peened, brazed, or spot welded to preclude removal. The term "2-inch square mesh of No. 9 wire" which meets the requirements of Federal Specification RR-F-191d, June 17, 1965, hereinafter shall be referred to as "wire mesh."

2. *Walls.* Construction should be of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other opaque materials offering similar resistance to or evidence of unauthorized entry into the area. If insert-type panels are used, a method should be devised to prevent the removal of such panels without leaving visual evidence of tampering. Area barriers up to a height of eight feet should be of opaque or translucent construction where visual access is a factor. If visual access is not a factor, the area barrier walls may be of wire mesh or other non-opaque material.

3. *Windows.* Window openings less than 18 feet above the ground or less than 14 feet directly or diagonally opposite uncontrolled windows in other walls, fire escapes, and roofs, shall be fitted with one-half inch bars (separated by no more than six inches), plus cross bars to prevent spreading, or wire mesh securely fastened on the inside. When visual access is a factor, the window shall be kept closed at all times, and shall also be translucent or opaqued by any practical method, such as paint on both sides of the window, tempered masonite, sheet metal, cement-asbestos board, etc. During nonduty hours the windows should be closed, and securely fastened to preclude surreptitious removal of classified material.

4. *Doors.* Doors shall be substantially constructed of wood or metal. When windows, panels or similar openings are used they shall be secured with wire mesh securely fastened on the inside. If visual access is a factor, the windows shall be translucent or opaqued. When doors are used in pairs an astragal (overlapping molding) shall be installed where the doors meet.

5. *Dood Louvers or Baffle Plates.* When used, they should be reinforced with wire mesh fastened inside the area.

6. *Door Locking Devices.* Entrance doors shall be secured with a built-in three-position, dial-type, changeable combination lock, or a three-position, dial-type, changeable combination padlock, as specified in paragraph 14a(3)(d). Other doors may be secured from the inside with a panic bolt, a dead bolt, a rigid wood or metal bar (which should preclude "springing"), extending across the width of the door and held in

DoD 5220.22-M

position by solid metal clamps, preferably fastened on the door casing, or other means approved by the cognizant security office.

7. *Ceilings.* Ceilings may be constructed of plaster, gypsum wallboard material, panels, hardboards, wood, plywood, ceiling tile, or other material offering similar resistance to and detection of unauthorized entry. Wire mesh may be used if visual access to classified material is not a factor. When wall barriers do not extend to the ceiling and a false ceiling is used, it should be reinforced with wire mesh. (This feature also applies when panels are removable and entry can be gained into the area without visible detection.) When such wire is used, an overlap molding secured by bolts should be used. (The bolts should be peened, brazed, or spot welded.) In those instances where barrier walls of an area extend to the ceiling, there is no necessity for reinforcing a false ceiling.

8. *Ceilings (Unusual Cases).* It is recognized that instances arise so that contractors may have a valid justification for no erecting a suspended ceiling as part of the area, especially in high-ceilinged hangers. The contractor may state that it is impractical to use a suspended ceiling because of his production methods, such as the use of overhead cranes for the movement of bulky equipment within the area. There are also cases wherein the

airconditioning system may be impeded by the construction of a solid suspended ceiling. At times, even the height of the classified material may make a suspended ceiling impractical. In such cases, special provisions should be made to assure that surreptitious entry to the area cannot be obtained by entering the area over the top of the barrier walls. Areas of this type should be closely scrutinized to assure that the structural safeguards are adequate to preclude entry via adjacent pipes, catwalks, ladders, etc.

9. *Miscellaneous Openings.* Where ducts registers, sewers, and tunnels are of such size and shape as to permit unauthorized entry, they should be equipped with man-safe barriers, such as wire mesh or, where more practical, steel bars at least one-half inch in diameter, extending across their width, with a maximum space of six inches between the bars. The steel bars should be securely fastened at both ends to preclude removal and should have crossbars to prevent spreading. When wire mesh or steel bars are used, care must be exercised to insure that classified material cannot be removed with the aid of any type instrument. Floor traps should be dead bolted inside the area. Care should be taken to assure that a barrier placed across any waterway (sewer or tunnel) will not cause clogging or offer any obstruction to the free flow of water or sewerage.

APPENDIX VI

EXTRACTS OF THE ESPIONAGE AND SABOTAGE ACTS AND OTHER FEDERAL CRIMINAL STATUTES

18 U.S. Code, Section 793. Gathering, Transmitting or Losing Defense In- formation

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its offices, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted, the same to any person not entitled to receive it, or willfully

retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever, having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to vio-

late any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

18 U.S. Code, Section 794. Gathering or Delivering Defense Information to Aid Foreign Governments

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or

by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

18 U.S. Code, Section 795. Photographing and Sketching Defense Installations

(a) Whenever, in the interests of national defense, the President defines certain vital military or naval installations or equipments as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

(b) Whoever violates this section shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

18 U.S. Code, Section 796. Use of Aircraft for Photographing Defense Installations

Whoever uses or permits the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment, in violation of Section 795 of this title, shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

18 U.S. Code, Section 797. Publication and Sale of Photographs of Defense Installations

On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under Section 795 of this title, whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp, or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

18 U.S. Code, Section 798. Disclosure of Classified Information

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

- (1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or
- (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

- (3) concerning the communication intelligence activities of the United States or any foreign government; or
- (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—

The term “classified information” means information which, at the time of a violation of this section is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms “code,” “cipher,” and “cryptographic system” include in their meanings, in additions to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings or communications;

The term “foreign government” includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term “communication intelligence” means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term “unauthorized person” means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

18 U.S. Code, Section 799. Violation of Regulations of National Aeronautics and Space Administration

Whoever willfully shall violate, attempt to violate, or conspire to violate any regulation or order promulgated by the Administrator of the National Aeronautics and Space Administration for the protection or security of any laboratory, station, base or other facility, or part thereof, or any aircraft, missile, spacecraft, or similar vehicle, or part thereof, or other property or equipment in the custody of the Administration, or any real or personal property or equipment in the custody of any contractor under any contract with the Administration or any subcontractor of any such contractor, shall be fined not more than \$5,000 or imprisoned not more than one year, or both.

18 U.S. Code, Section 2153. Destruction of War Material, War Premises, or War Utilities

(a) Whoever, when the United States is at war, or in times of national emergency as declared by the President or by the Congress, with intent to injure, interfere with, or obstruct the United States or any associate nation in preparing for or carrying on the

war or defense activities, or, with reason to believe that his act may injure, interfere with or obstruct the United States or any associate nation in preparing for or carrying on the war or defense activities, willfully injures, destroys, contaminates or infects, or attempts to so injure, destroy, contaminate or infect any war material, war premises, or war utilities, shall be fined not more than \$10,000 or imprisoned not more than thirty years, or both.

(b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.

18 U.S. Code, Section 2154. Production of Defective War Material, War Premises, or War Utilities

(a) Whoever, when the United States is at war, or in times of national emergency as declared by the President or by the Congress, with intent to injure, interfere with, or obstruct the United States or any associate nation in preparing for or carrying on the war or defense activities, or, with reason to believe that his act may injure, interfere with, or obstruct the United States or any associate nation in preparing for or carrying on the war or defense activities, willfully makes, constructs, or causes to be made or constructed in a defective manner, or attempts to make, construct, or cause to be made or constructed in a defective manner any war material, war premises or war utilities, or any tool, implement, machine, utensil, or receptacle used or employed in making, producing, manufacturing, or preparing any such war materials, war premises or war utilities, shall be fined not more than \$10,000 or imprisoned not more than thirty years, or both.

(b) If two or more persons conspire to violate this section, and one or more of such

persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.

18 U.S. Code, Section 2155. Destruction of National-Defense Materials, National-Defense Premises or National-Defense Utilities

(a) Whoever, with intent to injure, interfere with, or obstruct the national defense of the United States, willfully injures, destroys, contaminates or infects, or attempts to so injure, destroy, contaminate or infect any national-defense material, national-defense premises, or national-defense utilities, shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.

18 U.S. Code, Section 2156. Production of Defective National-Defense Material, National-Defense Premises or National-Defense Utilities

(a) Whoever, with intent to injure, interfere with, or obstruct the national defense of the United States, willfully makes, constructs, or attempts to make or construct in a defective manner, any national-defense material, national-defense premises or national-defense utilities, or any tool, implement, machine, utensil, or receptacle used or employed in making, producing, manufacturing, or repairing any such national-defense material, national-defense premises or national-defense utilities, shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.

18 U.S. Code, Section 371. Conspiracy to Commit Offense or to Defraud United States

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

50 U.S. Code, Section 797. Internal Security Act of 1950

(a) Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander desig-

nated by the Secretary of Defense, or by the Director of the National Advisory Committee for Aeronautics, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, water-front facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the Department of Defense, any Department or agency of which said Department consists, or any officer or employee of said Department or agency, or of the National Advisory Committee for Aeronautics or any officer or employee thereof, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse or other unsatisfactory conditions thereon, or the ingress thereto or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident or by enemy action, sabotage or other subversive actions, shall be guilty of a misdemeanor and upon conviction thereof shall be liable to a fine of not to exceed \$5,000 or to imprisonment for not more than one year, or both.

(b) Every such regulation or order shall be posted in conspicuous and appropriate places.

APPENDIX VII

GUIDANCE FOR PREPARATION OF DEFENSIVE SECURITY BRIEFINGS

A. General

A defensive security briefing containing elements of the following outline shall be given to those individuals or employees so identified in paragraph 5u.

B. Introduction

The following elements of information are intended to be neither all-inclusive nor all-exclusive, but should be used as source material in the preparation of briefings and as a guide for the type of information to be included in a briefing. Routine, stereotyped briefings not only fail to meet intended objectives, but could actually weaken security by giving the recipient false sense of security. Only the use of thoughtfully prepared briefings, based on the nature and extent of the classified information to which the proposed traveler has had access, the level of the office or position he occupies, and the scope and nature of the threat to which his proposed activity may expose him, will accomplish the purpose.

C. Rationale

United States policy favors interchanges with Communist countries by information and people provided the national security is not jeopardized. The U.S. has concluded exchange agreements with some Communist countries and conducts exchanges with others on an informal basis. United States citizens continue to be welcome to the Soviet Union and its satellite countries despite the various incidents which have tended to complicate official relations. However cordially they may be received, U.S. citizens who have had access to classified defense information are important targets for hostile intelligence services.

These services are constantly on the alert for opportunities to gain any kind of advantage that can be exploited, regardless of the country visited. It is the common practice of all intelligence services to establish and maintain current dossiers on personnel of intelligence interest. These dossiers reflect not only the names of key personages, but also the names of personnel whose jobs afford them access to vital defense information in any area of special interest.

D. The Communist Country Intelligence Network

1. The intelligence network of the Communist country is worldwide, wholly inclusive, and ever present. The principal control is the KGB. The title is deceiving as a description of the mission and power of this organization. It is directly responsible to the Soviet Council of Ministers for development and maintenance of internal security and all intelligence operations in countries of Soviet interest, with the exception of strategic intelligence, which is directed by the Defense Ministry.

2. Intelligence operations are hidden behind the immunity of embassies, consulates, trade delegations, missions and, in fact, any group that has contact with personnel who may be of intelligence interest. These intelligence agencies have concentrated on those fields which involve scientific and military knowledge possessed by the Western powers.

E. Techniques Employed to Obtain Information of Intelligence Value

1. One of the key sources of technical and scientific information is the numerous con-

ventions, seminars, conferences, and symposia held throughout the world each year. Many of these are open for attendance by representatives from all nations, including the Communist countries. These representatives are especially trained and extremely proficient in obtaining information they want without disclosing anything of significant value in return. Particular care must be exercised in the preparation of formal papers to be presented at meetings of this type and in participation on panels to insure that vital defense information is not disclosed. Another source is visits by representatives of Communist countries to military and other Government installations, industrial facilities, and other private institutions in the U.S. While these visits may be permitted for discussions on an unclassified basis, provided the nationals from these Communist countries do not have access to areas where classified work is being performed and it is determined that there is no risk of possible compromise of classified information through observation, contact with personnel engaged in classified work, or other means, nevertheless, extreme care must be taken in the conduct of such visits. No Communist country scientist is allowed to undertake foreign travel without approval of his government's intelligence service. In many instances, the individual Communist country scientist has received intelligence training, or is employed by the intelligence service on a project basis for the development of information in a particular area. The American host must be on his guard against attempts by his visitors to maneuver the conversation away from the stated purpose of the visit in order to obtain vital defense information.

2. Other means of obtaining information is through the tight, police-like controls over the movements of all foreign personnel visiting Communist countries. Guides and interpreters are members of, or cooperate with secret police agencies. In fact, the traveler may be "targeted" the moment he applies for a visa. Under such controlled conditions,

there is little that can be done to prevent espionage efforts and harassments directed against a selected individual. Intourist, Orbis, and other Communist travel agencies invariably arrange for American travelers to stay at the better class hotels, and there is evidence that, in many cases, the Americans are assigned rooms in which listening devices have been permanently installed. Eavesdropping is becoming more expert every day. Even now transistors as small as the head of a wooden match are taking over the jobs formerly performed by bulky radio tubes.

3. Another source of information is the personal mail of the traveler. All mail to and from the Communist countries is subject to censorship. The KGB and its counterpart agencies in the satellite countries examine the mail of American travelers from both a counterintelligence and positive intelligence point of view.

4. The American traveler should maintain a high level of personal behavior at all times. He should remember that he is a guest in a foreign country and a representative of the U.S. He should take extreme care to avoid revealing any information which might be of positive value to the Soviet or satellite intelligence collection effort. He should be temperate in his drinking. Aside from creating embarrassing or even scandalous scenes, the American, by overindulgence, may set himself up for possible compromise. Cases have been reported wherein inebriated persons have been maneuvered into sexual activities, which were photographed and used as a basis for blackmailing the individual into espionage. This is one of the oldest and most favored methods of compromising an individual.

5. Medical or dental service should be obtained from persons or institutions recommended by U.S. Consular officials. Drugs and anesthesia have been used under the guise of medical treatment for the purpose of aiding in interrogations. It is possible that they might be used by hostile intelligence to

obtain sensitive information from a foreign traveler or visitor.

6. While the techniques employed by Communist countries intelligence services seem far-fetched, illicit, or taken from "spy novels," they are in fact used in day-to-day activities and operations. Although these techniques are revolting to an American, he must nevertheless recognize them as part of the Communist system in order that he may successfully counter such practices.

F. Summary

In conclusion, it must be remembered that Communist countries intelligence and security services carry their espionage activities to fantastic lengths. Only the limits of the imagination curtail espionage services in developing new techniques, new concepts, and new targets. An individual's own lack of discretion or alertness gives these agencies the opportunities they desire. Be alert and:

a. *Don't*

- (1) Take classified information out of the U.S.
- (2) Discuss classified information outside of U.S. approved facilities.
- (3) Engage in blackmarket activities especially in the purchase of art treasures or the sale of currency.
- (4) Accept letters, photographs, packages, or any material to be smuggled out of the country for any reason.

- (5) Make statements which may be exploited for propaganda purposes.
- (6) Photograph military installations, other "restricted" areas or military personnel.
- (7) Get overly friendly with tourist guides, interpreters, or other citizens, particularly if they happen to know your special field.
- (8) Permit a representative of a Communist country during a visit to a defense facility to divert an unclassified discussion to one which would result in the release of advanced industrial and scientific technology, whether classified or unclassified, not otherwise available to the Communist countries.
- (9) Discuss with representatives of Communist countries unclassified technical data, unless the requirements of the ITAR have been complied with.

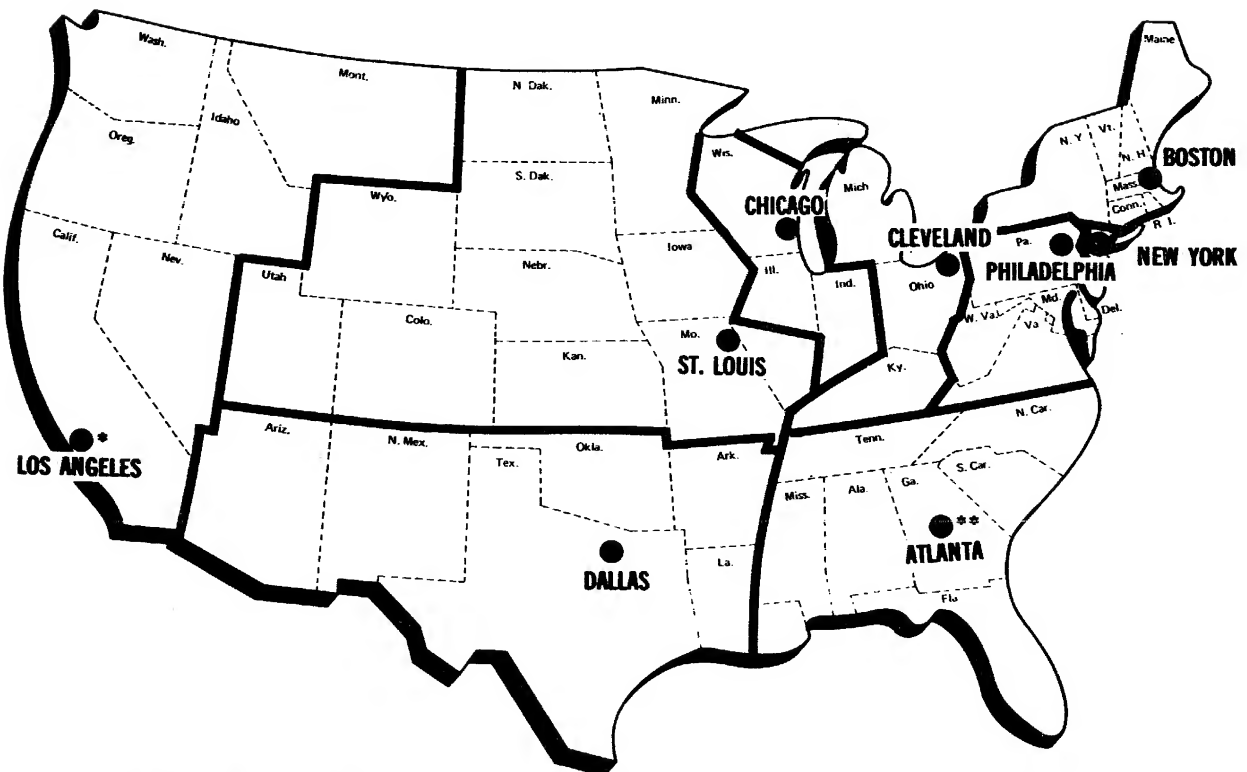
b. *Do.*

- (1) While abroad, report any apparent or suspected attempts at subversion to the U.S. Embassy of the country you are visiting, and in the U.S., report them to the nearest local office of the FBI.
- (2) Obtain medical or dental service from persons or institutions recommended by U.S. Consular officials when visiting foreign countries.
- (3) Remember you are an American citizen first, last and always.

APPENDIX VIII

INFORMATION REGARDING DCASRs, DISCO, DISI AND OISE ←

DEFENSE CONTRACT ADMINISTRATION SERVICES REGION BOUNDARIES



- * Includes Alaska and Hawaii and U. S. possessions and trust territories in the Pacific area
- ** Includes Puerto Rico, Panama Canal Zone and U. S. possessions in the Atlantic and Caribbean areas

OPERATIONAL AREAS OF DCAS COGNIZANT SECURITY OFFICES

Atlanta

The States of North Carolina, South Carolina, Georgia, Tennessee, Mississippi, Alabama, Florida, and the counties of Jefferson, St. Bernard and Plaquemines in Louisiana as well as any other territory in Louisiana which is East of the Mississippi River, Puerto Rico, Panama Canal Zone and U.S. possessions in the Atlantic and Caribbean areas.

Boston

States of Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, Connecticut and the following counties in New York:

Albany	Erie	Montgomery	Schuyler
Allegany	Essex	Niagara	Seneca
Broome	Franklin	Oneida	Steuben
Cattaraugus	Fulton	Onondaga	Sullivan
Cayuga	Genesee	Ontario	Tioga
Chautauqua	Greene	Orleans	Tompkins
Chemung	Hamilton	Oswego	Ulster
Chenango	Herkimer	Otsego	Warren
Clinton	Jefferson	Rensselaer	Washington
Columbia	Lewis	St. Lawrence	Wayne
Cortland	Livingston	Saratoga	Wyoming
Delaware	Madison	Schenectady	Yates
Dutchess	Monroe	Schoharie	

Chicago

The States of Wisconsin, Indiana and the following counties in Illinois.

Boone	Henderson	Logan	Schuyler
Bureau	Henry	McDonough	Stark
Carroll	Iroquois	McHenry	Stephenson
Champaign	Jo Daviess	McLean	Tazewell
Cook	Kane	Marshall	Vermilion
DeKalb	Kankakee	Mason	Warren
DeWitt	Kendall	Mercer	Whiteside
DuPage	Knox	Ogle	Will
Ford	Lake	Peoria	Winnebago
Fulton	LaSalle	Piatt	Woodford
Grundy	Lee	Putnam	
Hancock	Livingston	Rock Island	

Cleveland

The States of: Ohio, Michigan and Kentucky, plus Erie, Mercer and Crawford counties in Pennsylvania.

Dallas

The States of New Mexico, Texas, Oklahoma, Arkansas, Arizona and Louisiana less the counties of Jefferson, St. Bernard and Plaquemines and any other territory in Louisiana which is East of the Mississippi River.

Los Angeles

The States of: California, Alaska, Nevada, Washington, Montana, Oregon, Idaho, Hawaii, and U.S. possessions and trust territories in the Pacific area.

New York

The following counties in New York:

Bronx	New York	Putnam	Rockland
Kings	(Manhattan)	Queens	Suffolk
(Brooklyn)	Orange	Richmond	Westchester
Nassau			

The following counties in New Jersey:

Bergen	Hunterdon	Morris	Sussex
Essex	Middlesex	Passaic	Union
Hudson	Monmouth	Somerset	Warren

Philadelphia

States of Virginia, West Virginia, Delaware, Maryland, the District of Columbia, Pennsylvania (less counties of Erie, Crawford and Mercer) and the following counties in New Jersey:

Atlantic	Cape May	Gloucester	Ocean
Burlington	Cumberland	Mercer	Salem
Camden			

St. Louis

The States of Wyoming, Colorado, North and South Dakota, Nebraska, Kansas, Minnesota, Utah, Iowa, Missouri, and the following counties in Illinois:

Adams	Edgar	Lawrence	Pulaski
Alexander	Edwards	Macon	Randolph
Bond	Effingham	Macoupin	Richland
Brown	Fayette	Madison	St. Clair
Calhoun	Franklin	Marlon	Saline
Cass	Gallatin	Massac	Sangamon
Chrisian	Greene	Menard	Scott
Clark	Hamilton	Monroe	Shelby
Clay	Hardin	Montgomery	Union
Clinton	Jackson	Morgan	Wabash
Coles	Jasper	Moultrie	Washington
Crawford	Jefferson	Perry	Wayne
Cumberland	Jersey	Pike	White
Douglas	Johnson	Pope	Williamson

DCASR TELEPHONE NUMBERS AND ADDRESSES

The following listing contains the addresses and telephone numbers of all DCASRs and the currently available extensions of the Directorate of Industrial Security within each Region.

<i>City & State</i>	<i>Address</i>	<i>Area Code</i>	<i>Telephone Number</i>	<i>Directorate of Industrial Security Extension</i>
DCASR Atlanta, Ga. 30060	805 Walker St. Marietta, Ga.	404	424-6000	209
DCASR Boston, Mass. 02210	666 Summer Street	617	542-6000	804
DCASR Chicago, Ill. 60666	O'Hare International AP P.O. Box 66475	312	694-3031	6233
DCASR Cleveland, O. 44199	Federal Office Bldg. 1240 East 9th Street	216	522-5334	same
DCASR Dallas, Texas 75201	Merchandise Mart Bldg. 500 South Ervay Street	214	744-4581	270
DCASR Los Angeles, Calif. 90045	11099 S. LaCienega Blvd.	213	643-1082	same
→ DCASR New York, N.Y. 10013	60 Hudson St.	212	374-9040	same
DCASR Philadelphia, Pa. 19101	P.O. Box 7478 2800 South 20th Street	215	271-4030	same
DCASR St. Louis, Mo. 63101	1136 Washington Street	314	268-6311	same

In exceptional situations the following telephone numbers may be used to obtain verification of facility clearance and storage capability of prospective contractors and subcontractors. The request and verifying data must be confirmed in writing.

<i>DCASR</i>	<i>AREA CODE</i>	<i>TELEPHONE NUMBER</i>	<i>AUTOVON NUMBER (For Govt. Agencies Use)</i>
Atlanta	404	424-6000 x 209	697-9209
Boston	617	542-6000 x 838	955-8838
Chicago	312	694-3031 x 6232	930-6232
Cleveland	216	522-5338	580-5338
Dallas	214	744-4581 x 276	940-1276
Los Angeles	213	643-0203	833-0203
→ New York	212	374-9046	994-9046
Philadelphia	215	271-4035	444-4035
St. Louis	314	268-3567	698-3567

→ The following listing contains the addresses and telephone numbers of DISCO, DISI and OISE.

<i>City & State</i>	<i>Address</i>	<i>AREA CODE</i>	<i>TELEPHONE NUMBER</i>
DISCO, Columbus, OH 43216	P.O. Box 2499	614	236-2133 (Duty hours) 236-2058 (After hours) 850-2133 (Duty hours)
	<i>AUTOVON NUMBER (For Govt. Agencies Use)</i>		
DISI, Richmond, VA 23297	c/o Defense General Supply Center	804	275-4891
	<i>AUTOVON NUMBER (For Govt. Agencies Use)</i>		695-4891
→ OISE, Brussels	<i>Physical Address:</i> Office of Industrial Security, Europe, U.S. Defense Logistics Agency, 13 Chaussee de Louvain, 1940 St. Stevens Woluwe, Belgium <i>Mailing Address:</i> Office of Industrial Security, Europe APO New York 09667		Brussels, Belgium 720-8259

APPENDIX IX

PUBLIC INFORMATION SECURITY GUIDANCE

This Directive provides public information security guidance governing the public release of information by contractors holding DoD contracts. Questions by contractors as

to releasability of information should be referred to the Directorate of Security Review, OASD(PA).

18 January 1952
Number 5230.3

(Public Information Security Guidance No. 16)

DoD Directive

Washington, 25, D.C.

TITLE PUBLIC INFORMATION

by the Department of the Army, Navy and Air Force is requested.

SUBTITLE SECURITY REVIEW,
CLEARANCE

NUMBER 5230.3
Information Releases by
Manufacturers

V. *RELEASABLE AND NON-RELEASABLE INFORMATION*

I. *PURPOSE*

It is the purpose of this directive to provide public information security guidance governing the public release of information by manufacturers holding Army, Navy or Air Force contracts.

A. Manufacturers who receive from the Departments of the Army, Navy, Air Force awards of classified or unclassified contracts, letters of intent or supplemental agreements for production of military equipment or supplies or for increased production of materials now being produced may release to the public information of the following general nature concerning any individual contract without further specific clearance by the Department of Defense.

II. *AUTHORITY*

This directive is issued under authority granted in Directive 20.20-1, 27 July 1951, and is in conformity with Directive 250.17-2, 5 January 1952.

1. A statement that a contract (or letter of intent) has been received.

III. *DIRECTIVE SUPERSEDED*

This directive supersedes Directive 700-.05-3, 25 September 1951 (Public Information Security Guidance No. 15).

2. Type of item in general terms (i.e., aircraft of standard types, tanks, trucks, ammunition, clothing, etc.) provided that the designation of the item or equipment itself is not classified.

IV. *APPLICABILITY*

This directive is applicable to all agencies of the Department of Defense and the Departments of the Army, Navy and Air Force and to manufacturers who receive from the Departments of the Army, Navy and Air Force awards of classified or unclassified contracts, letters of intent or supplemental agreements for production of military equipment or supplies. Necessary dissemination of this directive

3. In the case of *unclassified* negotiated or formally advertised contracts, releases may include the name of the purchasing office, a brief description of the commodity or service, quantity, and dollar amount of the contract.

4. A statement that workers in certain fields are required. Number of additional personnel needed by the plant may be announced.

5. Subject to restrictions listed in this Guidance, a contractor may advertise for bids from prospective subcontractors for component parts or services in those cases where the subsequent contract itself will be unclassified.
 6. Information previously officially approved for release.
- B. Contractors will not release to the public information of the following nature concerning such contracts, unless specifically approved and cleared by the Security Review Branch, Office of Public Information, Office of the Secretary of Defense:
1. Production schedules, future planning on production schedules, or rates of delivery.
 2. Information on sources of supply, quantities and qualities of strategic or critical supplies and movements, assembly or storage of supplies or material.
 3. Information on sabotage attempts or plant security measures.
 4. Information on any research and/or development contracts.
 5. Information, including any photograph, sketch or plan concerning first models of weapons or equipment, outstanding production achievements, or performance of weapons or equipment.
 6. Information on material for shipment to allied governments under MDAP, NATO, etc.
 7. Movement of military aircraft. This restriction is applicable to all cases, including those where actual movement order is unclassified. This action is to reduce unauthorized disclosure of aircraft deliveries, modification and conversion programs.
 8. Movement of naval vessels, unless approved by the responsible commander.
 9. Classified information.
- C. A subcontractor or branch plant involved in military production programs may also release information subject to paragraphs A & B above, provided he does *not*:
1. Indicate he is the sole supplier.
 2. Indicate the percentage of the contractor's requirements he provides in terms of quantity or dollar value.
 3. Reveal rates of production or deliveries.
- D. Manufacturers outside the Continental United States may, after initial public release by the Secretary of Defense, release to the public information subject to the provision of this Guidance. For initial release the contracting agency should forward pertinent information regarding the contract, together with the manufacturer's proposed release, through the Departments of the Army, Navy, or Air Force, as the case may be, to the Secretary of Defense. The Office of Public Information will make the original release if appropriate.
- E. In order that manufacturers holding classified contracts may make state of business reports to stockholders, stock exchange, etc., the total company-wide dollar value of backlog may be released provided:
1. That only the Department of Defense total is used and not broken down by individual military service or item.
 2. That the release does not reveal the quantity or volume of individual orders.
 3. That the report is not made for periods of less than three months.

F. In case of doubt as to the releasability of information, contractors, factories, subcontractors, etc., may contact the Security Review Branch for advice, or may refer to the contracting agency.

FOR THE ASSISTANT TO THE
SECRETARY FOR PUBLIC IN-
FORMATION:

JOSEPH S. EDGERTON
Lt. Colonel, USAF
Chief, Security Review Branch
Office of Public Information

APPENDIX X

USE OF ESCORTS FOR CLASSIFIED SHIPMENTS

(Also applies to carrier custodians)

A. General

Escorts must be cleared to the level of the information involved. A sufficient number of escorts shall be assigned to the classified shipment to assure continuous surveillance and control over the shipment while it is in their custody.

B. Instructions and Operating Procedures

Specific written instructions and operating procedures will be furnished escorts prior to the shipment and should include, but not necessarily be limited to, the following:

1. General unclassified outline of the mission.
2. Name and address of persons, including alternates, to whom the classified matter is to be delivered.
3. Receipting procedures.
4. Means of transportation to be used and route to be used.
5. Duties of each escort during movement, during stops en route, and during loading and unloading operations.
6. Emergency and communication procedures.

C. Functions of An Escort

Escorts assigned for the protection of security shipments shall:

1. Conduct themselves throughout each security shipment operation in such manner that the security of matter entrusted to them will not be prejudiced through carelessness, inadvertence, or lack of vigilance. Intoxicants or drugs which may impair their judgment may not be used by escorts while assigned to a security shipment.

2. Possess identification cards as prescribed in paragraph 8 and carry them at all times while having custody of security shipments. These cards will be safeguarded and the loss of a card will be reported immediately to their company security supervisor.

3. Accept custody for the shipment by signing a receipt; and, release custody of the shipment to the consignee after obtaining a receipt from one of the consignee's employees who has been positively identified and who is cleared to at least the same level as the classified shipment.

4. Carry packages on the person, or in handcarried containers, until delivered to consignee whenever practicable. Such packages shall be kept under the constant surveillance of the escort who shall be in a physical position to exercise direct security controls over the material.

5. When accompanying classified material in an express or freight car, provide continuous observation of the containers and observe adjacent areas during stops or layovers.

6. When traveling in an escort car accompanying a security shipment via rail, keep the shipment cars under observation and detain at stops, when practicable and time per-

DoD 5220.22-M

mits, to guard the shipment cars and check car or container locks and seals. The escort car (after appropriate arrangements with the railroad) should be prepositioned immediately behind the car used for the classified shipment in order to enable the escort to keep the shipment car under observation.

7. Maintain liaison, as required, with train crews, other railroad personnel, special police and law enforcement agencies.

8. When escorting security shipments via motor vehicles, maintain continuous vigilance for the presence of conditions or situations which might threaten the security of the cargo, take such action as circumstances might require to avoid interference with continuous safe passage of the vehicle, check seals and locks at each stop where time per-

mits, and observe vehicles and adjacent areas during stops or layovers.

9. When escorting shipments via aircraft, provide continuous observation of plane and cargo during ground stops and of cargo during loading and unloading operations. The escort shall not enplane until after the cargo area is secured. Furthermore, the escort should preferably be the first person to deplane in order to observe the opening of the cargo area. Advance arrangements with the airline are required.

10. Notify the consignor by the fastest means available if there is an unforeseen delay en route, an alternate route is used or an emergency occurs. If appropriate and the security of the shipment is involved, also notify the nearest office of the FBI.

APPENDIX XI

REQUIREMENTS APPLICABLE TO THE HAND CARRYING OF CLASSIFIED DOCUMENTS ABOARD COMMERCIAL PASSENGER AIRCRAFT

A. General

Classified documents shall not be hand carried aboard commercial passenger aircraft unless authorized in writing by a cleared OODEP of the contractor, or when extenuating circumstances dictate, another responsible official of the contractor as approved by the cognizant security office. Hand carrying of classified hardware or other bulky packages aboard commercial aircraft is prohibited unless specifically approved by the cognizant security office. In either case, contractors are not authorized to carry classified material across international boundaries. (This does not preclude use of regularly scheduled non-stop flight on U.S. carriers between the U.S. mainland and Alaska, Hawaii, Puerto Rico, the Panama Canal Zone, or U.S. possessions or trust territories.) Current Government security measures pertaining to the control of hand-carried items aboard commercial passenger aircraft include the inspection of all hand-carried luggage, briefcases, and packages. The following requirements, established for the hand carrying of classified documents aboard commercial passenger aircraft are in addition to those in paragraph 17. These procedures apply to classified documents only. Instructions regarding classified hardware and other bulky packages shall be requested from the cognizant security office on a case-by-case basis. These procedures are not applicable to classified COMSEC or COMMUNICATIONS ANALYSIS information.

B. Approval

A cleared OODEP or other responsible official as approved by the cognizant security office shall issue written authorization for an

employee to hand carry classified documents aboard a commercial passenger aircraft after the OODEP has determined that (i) as the result of a rare and unusual situation an emergency exists, (ii) the necessary classified documents are not available at the destination point of the traveler, and (iii) the material cannot be transmitted by other authorized means in a timely manner. Where there is only one employee assigned at a facility, that individual may approve his own courier authorization letter provided the cognizant security office is preadvised and identified as the point of contact in the authorization letter for authenticity purposes.

C. Authorization Letter and Identification Card

The individual designated as a traveler shall possess written authorization (see paragraph B, above) to carry classified material, and give a picture identification card or badge meeting the requirements of paragraph 8.

1. The traveler shall have the original of the written authorization. A reproduced copy is not acceptable; however, the traveler shall have sufficient authenticated copies to provide a copy to each airline involved. The written authorization may contain a printed (or typed) endorsement for signature by the host official at destination if a round trip is foreseen. In addition, the written authorization shall:

- (a) Be on letterhead stationery of the contractor authorizing the carrying of the classified material.

DoD 5220.22-M

- (b) Give the full name of the traveler and, if not included on the identification medium specified in paragraph 2, below, the date of birth, height, weight and signature of the traveler.
- (c) Describe the type of identification the traveler will present upon request (e.g., ABC Corporation picture badge, No. 1234).
- (d) Describe the material being carried which is to be exempt from opening (e.g., three sealed packages, 9½" x 12½" x 2").
- (e) Identify the points of departure and destination.
- (f) Be dated and have an expiration date which may not exceed 7 days from date of issue.
- (g) Carry the name, telephone number, title and signature of the authorizing official. The telephone number will enable confirmation of the authenticity of the traveler authorization. When there is only one employee assigned to a facility, identification and telephone number of the cognizant security office will be provided for authenticity purposes.

2. Personal identification medium shall:

- (a) Be an identification card, badge or credential showing, as a minimum, the name and photograph of the holder. If descriptive data of the holder is not shown on the card, badge, or credential, the date of birth, height and weight of the holder shall be included in the written authorization in accordance with paragraph 1(b), above.
- (b) Carry the name of the employing contractor, or otherwise be marked to denote "contractor."

3. If the facility does not have and cannot develop the necessary identification medium, the contractor may request the cognizant security office to issue one.

4. When a traveler visiting a User Agency or another cleared facility is given classified material which must be hand carried via commercial passenger aircraft and the traveler has no endorseable traveler authorization from the employing contractor, it will be necessary for an authorized official at the activity being visited to determine whether the hand-carrying mission is required. Depending on this determination, the host official will provide and sign a traveler authorization on the host's letterhead stationery and make other arrangements necessary for the hand-carrying mission.

D. Preparation for Transmission — Packaging

The classified documents to be hand carried by the traveler are to be packaged as follows:

1. Double-sealed envelopes, together with the classified documents contained therein, shall be of a thickness which facilitates physical inspection at the airport screening station by flexing, feeling, weighing, etc., without the envelopes being opened. If the material to be hand carried involves a number of copies or pages, the material shall be sealed in separate double envelopes in order to facilitate physical inspection by airport security personnel without opening the envelopes.

2. The envelopes shall contain no binders, paper clips, or other metal which would inhibit processing through detection devices at the airport.

3. Caution should be used with respect to the carrying of photographic film because detection devices may include X-ray equipment which could damage certain films.

E. Records

In accordance with paragraph 17i, the contractor shall maintain at the facility a list of classified material hand carried by the traveler. All classified material shall be accounted for upon return of the traveler.

F. Briefings

The traveler hand carrying the classified documents shall be briefed not only on his overall responsibilities to safeguard classified material, but also the contents of this Appendix. The traveler should be reminded that the classified documents shall be in his personal possession at all times if proper storage at a U.S. Government activity or appropriately cleared contractor facility is not available. Overnight stopovers are not permissible unless arrangements are made in advance for overnight storage of the classified material in a U.S. Government installation or a cleared contractor facility.

G. Instructions to Traveler

The traveler carrying classified documents shall process through the airline ticketing and boarding procedure in the same manner as all other passengers, except for the following:

1. The traveler shall present himself at the screening station for routine processing. Should the envelope containing the classified documents be in a briefcase or other carry-on luggage, the briefcase or luggage shall be routinely offered for opening for inspection for weapons. The screening official should be able to inspect the envelopes by flexing, feeling, weighing, etc., without any requirement for opening the envelope.

2. In the event that the screening official is not satisfied, the traveler at that time shall inform the official that the envelopes contain classified documents and shall present the

authorization letter and identification card.

3. At that point, the screening official will process the envelopes with a detection device.

- (a) No alarm results, the envelopes require no further examination.

- (b) If an alarm results, the traveler shall not be permitted to board, and therefore is not subject to further screening for boarding purposes.

- (c) The traveler himself and all other items he may be carrying will be subject to routine screening.

4. When not in the personal possession of the traveler, classified material shall be stored in accordance with paragraph 14. Opening or reading the classified documents by a screening official is not permitted. If these measures do not permit boarding without opening the envelopes, the traveler shall not proceed further, but shall arrange with his facility for alternate means of transmitting the material. The traveler may not open or authorize the opening of envelopes under any circumstances. Any instances in which the envelopes have been opened shall be reported promptly to the facility's security supervisor who shall report the matter to the cognizant security office.

5. In the event the traveler is aboard a commercial passenger aircraft which is hijacked and lands in a foreign country, he shall conduct himself as follows:

- (a) If identification is required, he shall show appropriate civilian identification.

- (b) He shall not, under any conditions, volunteer that he has classified material in his possession.

- (c) If questioned or interrogated in a foreign country, common-sense judgment shall be used in making any response, but travelers shall not under

DoD 5220.22-M

any circumstances reveal classified information. He shall attempt to maintain physical possession of the classified material at all times.

- (d) Upon return to the U.S., report the incident to the facility security supervisor who shall report the matter to the cognizant security office.

INDEX

This index is provided as an aid in using this Manual

Abbreviations:

- Description, 11a
- Subjects and titles, 11a(9)

Access to classified information:

- Definition of, 3a
- Limitations, 5c, 14c
- Requirements for, 20a

*Accountability records, 12**ACDA*

- Classified information, 20c, 24a(1)(d), 24b, 31d(1)(d)
- User Agency, 1c

*Addressing mail and shipments, 17k**Administrative termination, 29**ADP System, definition of, 101b**ADP System Access, definition of, 101a**ADP System Security, definition of, 101c**Audit Trail, 103a(2), 109**Advanced Declassification Schedule, App. II**Advance shipping notice, 17c(5)(c), 17d(3)(d)**Agreement, long-term visits, 40**Alarm systems:*

- Approval, 35c
- Central station, requirements for 35a(1)(c)
- Direct connect, 35a(1)(a)
- Individual alarms, 14a(2)(c), 14a(4)(c), 35b(2)
- Material and installation, standards for, 35b
- Purpose, 35a
- Records, 35a(1)(c)5
- Response time, 35a(2), 35a(1)(c)4
- Supplanting, 35a(1)
- Supplemental, 35a(2)

*Alien (see immigrant alien), def., 3b**Alternate storage locations:*

- General, 15a
- Containers, 15d
- Controls, 15e
- Records, 15c
- Security clearance requirements, 15b

*Annual list of OODEPs, 22a(4), b(4), c(4), d(5)**Armed Forces Courier Service, 17b, 17e(5), 101a**APO mail channels, 17c(2), 17e(3)**Artwork, marking of, 11a(4)**Atomic Energy RESTRICTED DATA (see RESTRICTED DATA)**Authority, authorization for:**ADP System:*

- data transmission, 107
- dedicated mode, 106
- disconnect, 101
- multi-level resource sharing, 110
- operation of 5b, 100d
- subcontracting, 108

*Alarm system, 35c**Applying classification, 10d**Alternate storage, 15a**Armed Forces Courier Service, 17b, 17e(5)**Classification guidance, subcontractors, 60b**Controlled areas, 34c**Degaussing equipment, 19h**Destruction, 19b**Disclosure at meetings, 5q, 9e**Electromechanical devices, 36c**Interim clearances, 26d**Licensing agreements, 21b**Methods of destruction, 19c**NATO subcontracts, 98b**Procurement of filling cabinets, 14f**Public releases, 5o**Recordings and photographs, 11a(6)**Regrading of documents, 11c**Releases:*

- between subsidiaries, 72b
- intelligence information, 5c, 41e
- to foreign governments, 93, 94d

Removal of material:

- by visitors, 38b(3)
- to residences, 14e

*Reproduction, 18a**Retention of classified material, 5m, 64**Sales literature, publishing of, 5p**Secure electrical transmissions, 17d(1), 17c(4)**Security procedures, meetings, 5q, 9d**Subcontracts:*

- with Canada, 65
- with United Kingdom, 65
- from foreign contracts, 66
- involving TOP SECRET, 59a

*Termination of accountability, 12h**Transmitting:*

- NATO material, 88c
- material outside U.S., 17e, 93b
- TOP SECRET material, 5x, 13i, 17b

*Use of U.S. information on foreign contracts, 5h**Visits:*

- to contractors, 41
- involving NATO information, 52
- involving RESTRICTED DATA, 42
- to User Agency activities, 43, 44, 45

Authorized persons, 3c

DoD 5220.22-M

- Badges:*
 - Employees, 8a
 - Reporting, 8c
 - User Agency installations, 8d
 - Visitors, 8b
- Bank, use of for storage, 15*
- Bankruptcy, reporting of, 6a(4) (e)*
- Bid material:*
 - Disposition of, 5l
 - Destruction authority, 19b
 - Publication and distribution of, 5p(2)
 - Unsolicited, 10f
- Briefings (see security briefings)*
- Cancelling classifications, 11c*
- Carrier:*
 - Custodian, 3e, App. X
 - Qualified, 3az
- Central computer facility, definition of, 101d*
- Central memory units (see magnetic recordings)*
- Central station alarm system, 35a(1), 35b(2)*
- Certificates:*
 - Consultant, Type A, 68a
 - Destruction, 19e, 105g
 - Representatives of foreign interests, 20k
 - NATO briefing, 85d
 - NATO clearance, 55
- Charts, marking 11a(5)*
- Checks, security, 5j*
- Classified information, definition, 3g*
- Classified contracts:*
 - Definition of, 3f
 - Listing of, 5z
 - Reporting of, 6a(8), 6a(19)
- Classification authority, 10d*
- Classification guidance:*
 - Dissemination outside, CONUS, 10g
 - Distribution, required, 61
 - For subcontracts, 60
 - For User Agency contracts and programs, 1a
 - General, 10a
 - Producers, 10c
 - Retention, 10c
 - Unsolicited bids, 10f
 - When issued, 10b
- Classified waste, 19f, 80c, 105f*
- Clearance (facility):*
 - Advertising, 20f
 - Annual list, OODEPs, 22a(4), b(4), c(4), d(5)
 - Appendage to Security Agreement, 21a
 - Basis for, 21
 - Board resolutions, 20i
 - Certificate, foreign affiliation, 21a
 - Consultant, Type B, 69
 - Definition, 3ac
 - Distribution of DD Form 441, -1, 21a, 73
 - Exclusion action, 22a(2), c(1), d(3), e
 - Executive committee, 22a(2), c(1), d(3)
 - Licensing agreements, 21b
 - Multiple facility, 73
 - Parent-subsidiary, 72
 - Security Agreement, 21a
 - Temporary help suppliers, 74
 - Termination of, 5n
- Clearance (individuals):*
 - Access:
 - use of clearance for, 20c
 - limitation on, 30d
 - Administrative downgrading of TOP SECRET, 30
 - Administrative termination, 29
 - Age limitations, 20b
 - Application for, 26a, c
 - Assurance, security
 - application for, 99a
 - issuance of, 99a
 - reproduction of, 20f
 - termination of, 99a(5)
 - Basis for, 20a
 - Concurrent, 26g
 - Conversion of, 27
 - Contractor clearances, criteria, 24b(1)
 - Duration, 20h
 - ERDA, 26l
 - Foreign nationals, 20l
 - Formerly cleared, 26i
 - Granted by:
 - DoD, 24a
 - contractor, 24b
 - Guards, 20e
 - Immigrant aliens, 20m, 24a(2), 26b
 - Interim clearances, 26d
 - Leave of absence, 20h
 - Letter of Consent:
 - issuance of, 26k
 - overseas assignment, 96
 - reproduction of, 20f
 - Multiple facility, 20d
 - Name change, 26j
 - Negotiators, 23
 - New clearances, 26c
 - Number of, 20j
 - Outside program, 20n
 - Preemployment clearance action, 25
 - Reciprocal, 31
 - Records, 28
 - Reemployment, 26h
 - Reinstatement of TOP SECRET, 30
 - Representatives of foreign interest, 3bb, 20k, 22f
 - Required clearances:
 - corporations, 22a

- sole proprietorships, 22b
- partnerships, 22c
- colleges and universities, 22d
- Revocation, 24c
- Signature, witness to, 24b (3), 26a
- Transfers, 26e, f
- Withdrawal, 20o
- Closed Areas: (see controlled areas)*
- Closed vehicle, 3i*
- Coding of badges and cards, 8a*
- Cognizant Security Office, 3j*
- Colleges and Universities, 3k*
- Combinations:*
 - Access to, 14c
 - Changing, schedule for, 5i
 - Classifying, 5i
 - Door devices, 36b
 - Knowledge of, 14c
 - Padlocks, security, 5i
 - Personnel authorized to change, 5i
 - Security enclosures, 36a
- Commercial Carrier, 17c (5), 17d (3)*
- Communication Intelligence, 3m*
- COMMUNICATIONS SECURITY (COMSEC)**
 - Briefing and debriefing, 5g
 - Clearances 24a (1) (a), (2), 24b
 - COMSEC Supplement, 76
 - Definition, 3n
 - Destruction, 19b (2)
 - Violations:
 - investigation of, 7d
 - reporting, 6a (3)
 - Communist relationships, 5v, 6b (4)*
 - Compilations, marking of, 11a (14)*
 - Complex, definition of, 14a (4) (a), 101e*
 - Compromise or suspected compromise:*
 - Definition, 3o
 - Investigation of, 7
 - Reporting, 6a (2)
 - Computer tapes, magnetic:*
 - Degaussing, 19h, 104, 105
 - Marking, 11a (7)
 - CONFIDENTIAL material:**
 - Clearances for access to, 24b, 26d, 26i
 - Definition, 3p
 - Destroying, 19d
 - Preparation for transmission, 17a
 - Receipts, 12e (2)
 - Records, 12a
 - Storage, 14a (5)
 - Supplemental controls, 14a (5)
 - Transmission within a facility, 17a (3)
 - Transmission outside a facility, 17d
 - Consignee, 3g*
 - Consignor, 3r*
 - Consultants:*
 - Letter agreement, 70a
 - Type A, 68
 - Type B, 69
 - Type C, 70
 - Under Civil Service procedures, 71
 - Contained, definition, 101f*
 - Containers (see storage)*
 - Continued classification after public release, 10h*
 - Continental United States, definition, 3s*
 - Contract Security Classification Specification, 10a, 60, 61*
 - Contracting Officer, 3t*
 - Contractor, definition of, 3u*
 - Contractor granted clearances, 24b*
 - Administrative Termination of, 29a, d
 - Control station personnel, 12d*
 - Control station records:*
 - Accountability, 12a
 - Destruction, 19e
 - Inventory lists, 17i
 - Production, 12f
 - Production control, 78
 - Receipts, 12g
 - Receipts and dispatch, 12c
 - Reproduction, 18c
 - Controlled Areas:*
 - Approval for, 34c
 - Basis for, 33
 - Closed Areas:*
 - construction, 34a, App. V
 - definition, 3h
 - identifying, 34a (4)
 - nonworking hours, 34a (3)
 - working hours, 34a (2)
 - Reports, 6a (5), 34d
 - Restricted Areas:*
 - definition, 3bc
 - Identifying, 34b (4):
 - nonworking hours, 34b (2)
 - working hours, 34b (1)
 - Courier, 17c (3), App. X*
 - Cover sheets, 11a (4), 78*

Covering:

Documents in use, 16b
Equipment, 17a(1)(c)

Credentials:

Recovery of, 8a(5)
Verifying, 8a(6)

CRYPTOGRAPHIC (CRYPTO)

Accounting for, 12a
Definition, 3v
Inventory/accounting 12b
Production of, 12f
Reproduction, 18a

Dates, required on classified material, 11a

DoD technical information dissemination activities, 5y

Declassify, definition of, 3w, App. II

Dedicated mode, definition, 101g

Definition of terms, 3

Degaussing, 19h, 105a

Delay in shipment, 6a(10), 17c(5)(c), 17d(3)(d)

Design features, incorporation of, 5h

Designation, applying:

To controlled areas, 34a(4), 34b(3)
To production areas, 11a(8)

Destruction:

Authorization, 19b
Certificates, request for, 19h, 105
Classified waste, 19f, 105
Destroying official, 19d
Equipment approval, 19c
Inspection of equipment, 19c
Magnetic recordings, 19h, 105
Methods, 19c, 105
Records and certificates, 19e, 105
Rented or leased equipment, 19c, 108b
Reproduction materials, 80, 81
Requirement of, 19a
Subcontractor employee, use of, 19c, d
Witness, 19d

Determining need-to-know, 5f

Direct-connect alarm system, 35a(1)

Discs and drums, declassifying, 104, 105

Discussion of classified information:

Recording of, 38b(2)

Disclosures:

At meeting, 5q, 9e
General, 5c
To subcontractors, 58a, 59

Disconnect, definition, 101h

Dispatch records, 12g

Disposition of classified material, 5l

Documents

Definition of, 3w
Marking of, 11a(1)

Downgrade, definition, 3z, App. II

Clearances, TOP SECRET, 30

Electrical transmission, 17b, 17c(4), 17d(1), 107

Electro-mechanical devices:

Approval, 36c
Door devices, 36a(2)
Security enclosures, 36a(1)
Supplemental, 36b

Electronic devices:

Approval, 36c
Door Devices, 36a(2)
Security enclosures, 36a(1)

Employee badges, 8a

Emergency procedure, 5w

ERDA facilities, visits to, 46

Escorts:

Definitions of (ADP), 101i
For transmission, 17c(3), App. X
For visitors, 38b(1)

Executive committee, 22a(2), c(1), d(3)

Executive personnel, 3aa

Exclusion of personnel, 5e

Facility, 3ab

Facility security clearance (see clearance)

FBI:

Reporting to, 7b(1)
Visits by, 41j

File folders, marking of, 11a(13)

Files, bulk, 11c(3)

Files, classified, 11a(13)

Fingerprints, 26a(4), (5)

Foreign:

Classified contracts, App. III
Classified information, 3ad
Interest, 3ad 1
Nationals, 3ae
Ownership, control & influence, 21c, 72a, App. 1
Representatives of foreign interest, 3bb
Travel, 5u, 6a(13)

FORMERLY RESTRICTED DATA:

Definition, 3af
Dissemination, 17l
Marking, 11b(3)

General Declassification Schedule, App. II

General requirements, 5

Graphic arts, definition of, 3ag (see reproduction)

Groups of documents (see files, classified)

Guards:

Clearance of, 20e
Emergencies, use of, 5w(1)
Entry control:
 alternate entrances, 36a(6)
 Closed Areas, 34a(2)
 facility complex, 14a(4)(a)
 meetings, 9d(4)
 room, building, structure, 14a(2)(a), 14a(4)(a)
 safe deposits area, 15d(4)

Patrols:

of Closed Areas, 34a(3)
of room, building, structure, 14a(2)(b), 14a(4)(b)
of strongrooms, 14a(3)(f)
Response to alarms, 35a(1), (2)

Subcontract:

Destruction of CONFIDENTIAL waste, 19f
Witness to destruction, 19d

Guides, classification, 10a, 58

Hardened container, 3ah, 17a(2)(a)

Home office, 3ai

Identifying facility of origin, 11a

Immigrant alien:

Clearance of, 20m, 24a(2), 26b, 26c(2)
Definition, 3aj

Individual responsibility for safeguarding, 5f

Information, definition of, 3al

Intelligence, 3am

International Traffic in Arms Regulations 21b, 41d, 48a(3), 50

Interpretations, requests for, 4

Inventory, in connection with visits, 17i

Inventory/Accounting of classified material, 12b

Investigations:

By Government representatives, 5aa
By contractors, 7

Investigative assistance, 5aa

Legends, marking, 11a(5)

Letters of transmittal, 11a(3)

Limitations on:

Destruction, 19b
Reproduction, 18a, 87a

List of classified contracts, 5z

Location of meetings 9c

Locked Entrance:

Closed Areas, 34a(2)(b), (3)
Definition, 3an
Room, building, structure, 14a(2)(a), 14a(4)(a)

Long-term visits, 40

Machine accounting cards, marking of, 11a(11)

Machine listings, marking of, 11a(10)

Magnetic recordings 19h

Magnetic tapes, degaussing of, 104, 105

Maps, marking of, 11a(5)

Markings:

Abbreviations, 11a
Artwork, 11a(4)
Blankets, 80f(2)
Bulk files, 11c(3)
Charts, 11a(5)
Compilations, 11a(14)
Containers (transmission), 17a(1)(e), 17a(2)(b)
Cover sheets, 78
DDC documents, 11c(2)
Documents, 11a(1)
Downgrading/declassification, 11b(5), App. II
Drawings, 11a(5)
Facility of origin, 11a
Files, 11a(13)
Films, 11a(6)
Foreign classified material, 11d
FORMERLY RESTRICTED DATA notation, 11b(3)
Letters of transmittal, 11a(3)
Linecasting machines, 79b
Machine-accounting cards, 11a(11)
Machine listing, 11a(10)
Magnetic recordings, 11a(7)
Maps, 11a(5)
Material, 11a(8)
Messages, 11a(12), App. II
Microfiche, 11a(6)
Microfilm, 11a(6)
Origination date, 11a
Overlays, 11a(4)
Pages, 11a(2)
Paragraphs, 11a
Photocomposition machines, 79b
Photographs, 11a(6)
Plates, reproduction, 80f(2)
Presses, reproduction, 79a

Production control records, 78
Recordings (sound, magnetic, other), 11a(7)
Regraded material 11c
RESTRICTED DATA notation, 11b(2)
Rolled or folded documents, 11b(4)
Sensitive Intelligence Information, 11b(4)
Subjects, 11a(9)
Titles, 11a(9)
Tracings, 11a(5)
Translations, 11a(15)
Working papers, 11a(16)

Mechanical Devices:

Approval, 36c
Door Devices, 36a(2)
Security enclosures, 36a(1)

Meetings, conducted by:

Contractors, 5q(1), (3)
DoD, 5q(2)
Other User Agencies, 5q(4)

Multi-level security mode, definition, 101j

Multiple facility organization:

Classification guidance, 73
Collocated facilities, 72c
Concurrent clearances, 20j
Definition, 3ap
Exchange of employee rosters, 37j
Interchange of classified information, 73, 72c
Personnel clearances, 20d(2), 26k
SPP, 5s, 73, 72c
Transfers, 26f
Visits between, 73, 72c

National of U.S., 3aq

NATO classified information:

Access record, 85b
Briefing, 85c
Clearances, 24a(1), 55, 86
Combination, changing of, 5i
Contracting officer functions, 89
Definition, 3ar
Destruction, 19b(4)
Marking, 87b
NATO officer, 85a
Reporting receipt of, 90
Reproduction, 87a
Subcontracting, 91
Transmission:
 within U.S., 88b
 outside U.S. 88c, d
Visits involving, 52, 53
Visits records, 54

Need-to-know definition of, 3as

Negotiator, definition of, 3at

Notations:

Downgrading or declassification, 11b(5), App. II
Exempt, App. II
Excluded, App. II
FORMERLY RESTRICTED DATA 11b(3)
RESTRICTED DATA, 11b(2)
Sensitive intelligence information, 11b(6)
Unauthorized disclosure, 11b(1)

Nuclear Weapon Security Program, 3at. 1

Office of Industrial Security, Europe, 95

Officers, definition of, 3au

Official information, 3av

Operating System, definition, 101k

Orientation of personnel, 5f, g

Overseas operations, 92, 93, 94, 95, 96, 97

Packaging classified material, 17a(1)

Paragraphs, marking, 11a

Parent-subsidiary:

Clearance requirements, 72a
Collocation of facilities, 72c
Exclusion action, 72a
Interchange of classified information, 72b

Patentable material, 5m(2)

Patrols, patrolling:

Closed Areas, 34a(3)
Facility complex, 14a(4) (b)
Rooms, buildings, structures,
 14a(2) (b), (4) (b)
Strongrooms, 14a(3) (f)

Personnel:

Authentication of, 106b(3)
Authorized to apply classification, 10e
Clearances (see clearance (individual))
Exclusion, 5e
Identification, 8
Photographs, marking of, 11a(6)
Suspected Compromise, investigation of, 7

Possessions, 3aw

Preparation for transmission, 17a(1), (2)

Principal management facility, definition, 3aw.1

Printing (see reproduction)

Production of classified materials:

Incorporation of, 12f(4)
Other material, 12f(3)
SECRET documents, 12f(2)
TOP SECRET, CRYPTO and Special Access
documents, 12f(1)

Proofs, 80b

Protective Security Service 3ax;
17a(2) (b), (d); 17c(5) (b)

Public release, 5o, App. IX

Pulping (for destruction), 19c

Qualified carried, 3ay, 17c(5)

Receipts:

Inner containers, inclusion, 12g(2),
17a(1)
Obtained during visits, 17i
Retention of, 12g(3)
Signing and return of, 12e(2)
Suspense file and follow-up, 12g(3)
Within a facility, 13d

Receipt and dispatch records, 12c

Receipt of classified material, 12e

Records of:

Accountability, 12a
ADP operating system tests, 103
Alternate storage facilities, 15c
Audit trail, 109
Badges and identification cards, 8a(5)
Clearances, 28
Combinations, knowledge of, 14c
Control cards, electronic, 36a, b
Destruction, 19e
Discussions and photographs, 38b(2)
Inventory accounting, 12b
Inventory, visits, 17i
NATO access, 85b
NATO visits, 54
Production control, 78
Receipt and dispatch, 12c
Reproduction, 18c
Retention of, 5m
TOP SECRET access, 13a
Visitors, 39

Reference Material, 3az

Registered mail, 17c, d(2), (3), (4); 88b

Registry, Central, 87a, 88c, 90

Regrading:

Authority, 11a, App. II
Definition, 3ba
Marking, 11c

Release of classified information, 5x

Remote terminal, definition, 101l

Removal of classified material to residence, 14e

Reports, reporting:

Adverse information, 6b(1)
Annual reports of OODEPs, 6a(17)
Assignment of immigrant aliens, 6b(6)
Attendance at Meetings, 5u(1)
Authorization to apply classifications, 6a(14)

Badges and identification cards, 6a(13)

Category of classified information, 6a(8)

Changed conditions, 6a(4)

Change in Closed or Restricted Area 6a(5)

Change in employee's status, 6b(2)

Change in storage capability, 6a(6)

Delay in shipment, 6a(10)

Employee information in compromise cases, 6a(7)

Espionage, sabotage, or subversive activities,
6a(1)

Evidence of tampering, 6a(11)

Foreign classified contracts, 6a(18)

Improper shipment, 6a(12)

Inability to safeguard classified material, 6a(16)

Location or disposition of classified material, terminated from accountability, 6a(15)

Loss, compromise or suspected compromise, 6a(2)

Official investigation, 6b(3)

Official security violations, 6a(3)

Relationships in Communist countries, 6b(4)

Representative of a foreign interest, 6b(5)

Termination statement, 6a(9)

Travel or Attendance at Meetings, 5u(1)

Reproduction:

Area controls:

bindery areas, 79c
composition areas, 79b
darkrooms, 79d
pressrooms, 79a
proofreading areas, 79e
shipping entrances, 79f

Authorizations for, 18a

Blankets, rubber, 80f(2)

Blankets, other than rubber, 80f(3)

Bulk shipments, 80e

Designation of equipment, 18

Destruction, special requirements, 81

Identification of:

linecasting machines, 79b
photocomposition machines, 79b
presses, 79a

Mailing lists:

classified, 82a
unclassified, 82b

Overruns, 80h

Plates, 80f(2)

Press, parts of, 80f(4)

Production material, 80f(1)

Proofs, 80b

Records:

control station, 18c
production control, 78
Regraining of plates, 80f(2)
Samples, return of, 80d
Waste, disposal of, 80c

Resource-Sharing Computer System, definition, 101m

Restricted Areas: (See Controlled Areas)

RESTRICTED DATA:

Clearance for access to, 24a
Definition, 3bd
Dissemination, 17l
Marking, 11b(2)
Violations involving, 7d
Visits involving, 42

Retention of classified material:

General, 5m
By subcontractors, 64

Return of classified material, 5l, 64, 80d

Return of receipts, 12e(2)

Rolled and folded documents, 11b(6)

Safeguarding:

General, 5d
Individual responsibility, 5f

Safeguarding U.S. information overseas:

Custody, 94c
Disclosure, 94d
Storage, 94c
Transmissions, 94b

Safeguards during use, 16

Sales literature, 5p

SECRET material/information:

Accounting for, 12a
Authority for:
 disclosure at meetings, 9e
 removal to residence, 14e
 reproduction, 18a
 transmission, 17e
Clearance for access to, 24a, 26d, 26i
Definition, 3bf
Destruction of, 19d, e
Inventory/Accounting, 12b
Preparation for transmission, 17a
Production of, 12f
Receipts for, 12g, 17a
Storage:
 containers, 14a(3)
 supplemental controls, 14a(4)
Transmission:
 by commercial carrier, 17a(2)
 method, 17c
 outside U.S., 17e
 preparation for, 17a(1)
 within a facility, 17f

Security, definition of, 3bg

Security Agreement:

Execution of, 21
Termination of, 5n
Security Assurance, 99, 20f

Security Briefings:

Destruction official, 19d
Defensive, 5u, App. VII
Individual responsibilities, 5f
NATO, 85c
Overseas assignment, 96
Refresher, 97c, d
Security briefing and termination, 5g
TOP SECRET, 13b
Visitors, Category, 5, 41e
Visitor escorts, 38b

Security checks, 5j

Security cognizance, 1d, 3bh

Security enclosures, 36a

Security of combinations, 5i

Security supervisor, 5a, 7a, 102b

SENSITIVE COMPARTMENTED INFORMATION

Clearances 24a(1)(a), (2), 75d
Contracts, 75
Definition, 3bh.1

Sensitive Intelligence Information, 11b(4)

Shredders, 19c

Shipments:

Bulk, 80e
SECRET, controlled, 3bf

Shipper, 3bi

Short title, 3bj

Signature Security Service, 3bk, 17d(3)

Signing receipts, 12e

Single Line Service, 3bl

Software definitions, 101n

Special Access Programs, 3bm, 5t

Sponsored meetings:

Attendance of foreign nationals and representatives of a foreign interest, 9b
Location of, 9c
Requests for, 9a
Requests for attendance, 9f
Requests for disclosure authority, 9e
Security procedures for, 9d

Standard Practice Procedures, 5s, 5w 19c(4), 73, 102a

Standards, Underwriters' Laboratories, 35

Strongrooms, 14a(3)(f), App. IV, F.

Storage:

Alternate storage locations, 15
Bulky material, 14b
classified waste, 19f
CONFIDENTIAL material, 14a(5)
Desk pedestals, 14a(3)(g)
En route to destination, 17h

DoD 5220.22-M

GSA approved cabinets, 14a(1), (3)(a)
 Lock bar, security of, 14a(3)(g)
 Overseas, 94c
 Private residence, 14e
 Protection during non-working hours, 14d
 SECRET material, 14a(3), (4)
 Steel file cabinets, 14a(3)(d)
 Supervision of containers, 14c
 Supplemental controls for:
 SECRET material, 14a(4)
 TOP SECRET material, 14a(2)
 TOP SECRET material, 14a(1)
 Vaults:
 Class A, 14a(1), App. IV
 Class B, 14a(3)(b), App. IV
 Class C, 14a(3)(c), App. IV

Subcontractors:
 Approval of requests from, 56
 Badging, of, 8a(7)
 Classification guidance, 60
 Clearance status of, 58
 Disclosure of TOP SECRET to, 59a
 Distribution of guidance, 61
 Restrictions:
 for changing combinations, 5i
 for destruction purposes, 19c, 80f(2)
 Return of classified information, 64
 Safeguarding ability of, 59
 Selection, notification of, 62
 Subcontract Classified Data Processing, 108
 Subcontracting on foreign contracts, 66
 Subcontracting with foreign industry, 65
 Telephone requests, regarding, 59b(4)
 Unsatisfactory conditions at, 63
 Visit requests for, 41a(3)

Subjects and titles, marking of, 11a(9)

Subsidiary, 3bn

Supplanting alarm systems, 35a(1)

Supplemental alarm systems, 35a(2)

Tape recordings, 11a(7)

Temporary help suppliers, 74

Termination of accountability, 12h

TOP SECRET material/information:
 Access records, 13a
 Accounting for, 12a, 13e
 Authority for:
 disclosure at meetings, 9e
 disclosure to subcontractors, 59a, 13j
 removal to residence, 14e
 reproduction, 18a, 13h
 transmission, 13i, 17b
 Clearance for access to, 24a; 26d, i
 Control station personnel, 12d

Definition, 3bp
 Destruction of, 19e
 Dissemination, 13c
 Inventory/accounting, 12b, 13g
 Preparation for transmission, 17a
 Production of, 12f
 Receipts for, 12g, 13d, 17a
 Reproduction, 13h
 Restriction, ADP, Logic Disconnect, 101h
 Security Assurance, issuance of, 99b
 Special Requirements, 13
 Storage:
 containers, 14a(1)
 supplemental controls, 14a(2)
 Transmission:
 method, 17b
 preparation for, 17a(1)
 within a facility, 17f
 Violation, involving, 7d

Tracing Receipts, 12g(3)

Transfer of employees, 26e, f

Translations, marking of, 11a(15)

Transmission, ADP, definition, 103o

Transmission:
 Additional protection during visits, 17i
 Additional requirements, commercial carriers, 17a(2)
 Addressing mail or shipments, 17k
 ADP Data, 107
 Inspection of classified mail and shipments, 12e, 17g
 Method of transmitting:
 ADP, approval for, 106, 107
 COMSEC material, 17j
 CONFIDENTIAL material outside facility, 17d
 NATO material, 88
 outside U.S. and possessions, 17e, 94b
 SECRET material outside of facility, 17c
 SECRET and CONFIDENTIAL material within a facility, 17f
 TOP SECRET material outside facility, 17b
 TOP SECRET material within facility, 17f
 Preparation for:
 outside a facility, 17a(1)
 within a facility, 17a(3)
 Protection en route, 17h
 Report of evidence of tampering, 6a(11)
 Restriction for RESTRICTED DATA, 17l

Transmittal letters, 11a(3)

Transshipping, 3bg, 17c(5)(c)

Trust territory, definition of, 3br

Type A Consultants, 68

Type B Consultants, 69

DoD 5220.22-M

Type C Consultants, 70
Unauthorized Disclosure Notation, 11b(1)
Unauthorized person, 3bs
United States, definition of, 3bt
Upgrading:
 Definition of, 3bu
 Method, 11c
Unsolicited proposals, 5p(2), 10f
Unsponsored meetings, controls over, 5q
User Agencies, 3bv
Vaults and strongrooms:
 Class A, 14a(1), App. IV
 Class B, 14a(3)(b), App. IV
 Class C, 14a(3)(e), App. IV
 Strongrooms, 14a(3)(f), App. IV
Visitor badges, 8b
Visits:
 Advance notice, 37d
 Authority for, 37e(4)
 Briefing, 41c
 Carrying classified material on 17e, f
 Categories:
 1. 41a
 2. 41b
 3. 41c
 4. 41d
 5. 41e
 Control of, 38b
 Criteria for approval, 37b
 Disapproval notice, 37c
 Escorts, 38b, 101i
 Facility clearance, verification of, 38a
 Identification of visitor, 38a
 Involving RESTRICTED DATA, 42
 Long-term, 40
 Multiple facility organization, 73
 NATO visits:
 clearance certificate, 55
 definition of, 39
 records of, 54
 recurring, 52d
 NPLO programs, 53
 Processing time, 49
 Recordings and discussions, 38c
 Records of, 39
 Recurring, 37f
 Removal of classified material during, 38d
 Requests, contents of, 37d, 41
 Telephone requests regarding, 37d
 Under bilateral agreements, 51
 Use of OISE for, 50
Visits to:
 Activities other than ERDA, 47
 ERDA and its contractors, 46
 Foreign Governments and Activities, 48
 User Agencies in the U.S., 44
 User Agencies outside the U.S., 45
Waste material, 19f, 80c
Weapon system, definition of, 3bw
Witnesses for destruction, 19d
Working hours, definition of, 14a(2)
Working papers, 12f, 11a(16)